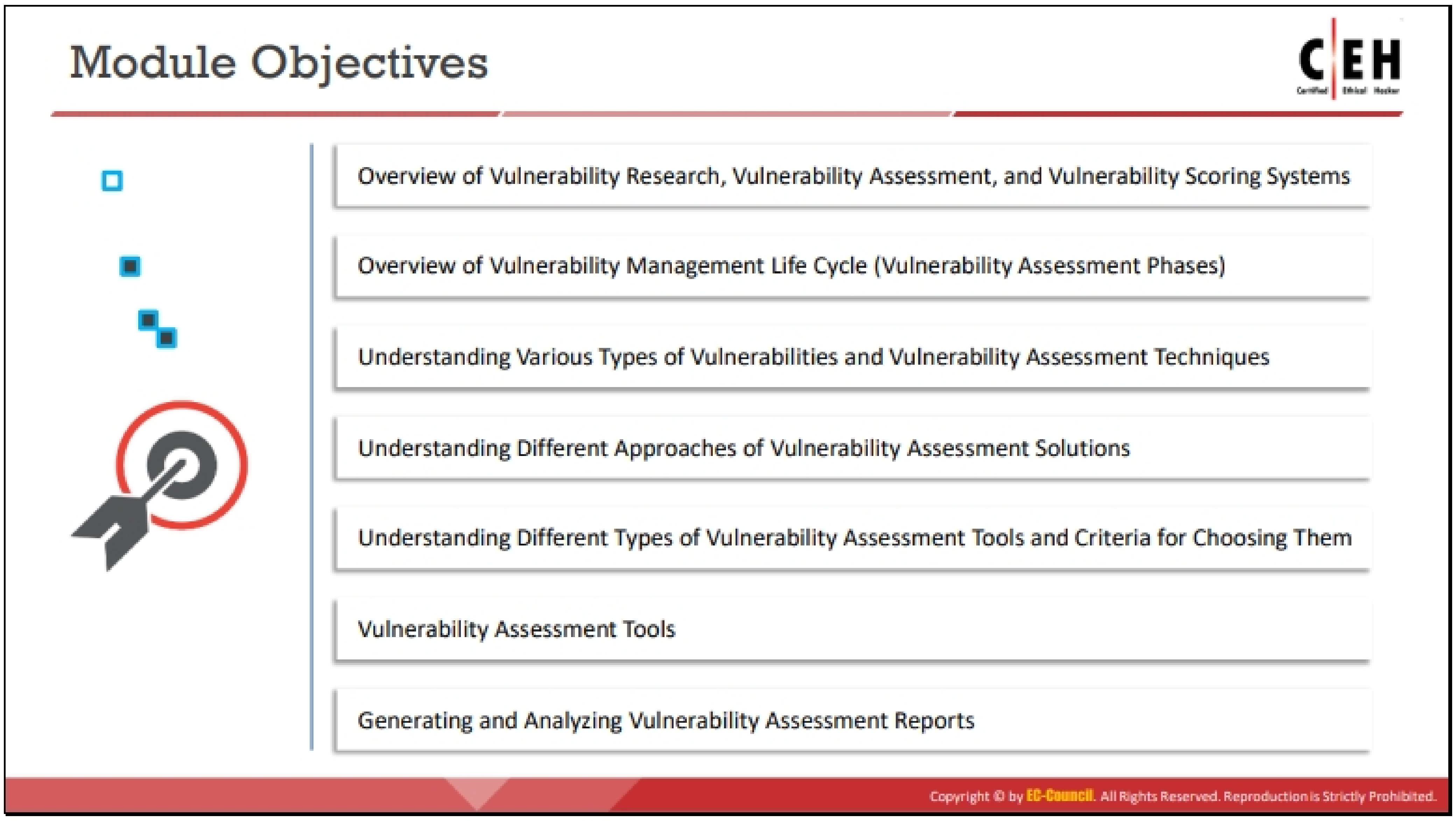
C|EH™
Certified Ethical Hacker

Module 05:
Vulnerability Analysis



Module Objectives

- Overview of Vulnerability Research, Vulnerability Assessment, and Vulnerability Scoring Systems
- Overview of Vulnerability Management Life Cycle (Vulnerability Assessment Phases)
- Understanding Various Types of Vulnerabilities and Vulnerability Assessment Techniques
- Understanding Different Approaches of Vulnerability Assessment Solutions
- Understanding Different Types of Vulnerability Assessment Tools and Criteria for Choosing Them
- Vulnerability Assessment Tools
- Generating and Analyzing Vulnerability Assessment Reports

Module Objectives

In today's world, organizations depend heavily on information technology for protecting vital information. This information is associated with areas of finance, research and development, personnel, legality, and security. Vulnerability assessments scan networks for known security weaknesses.

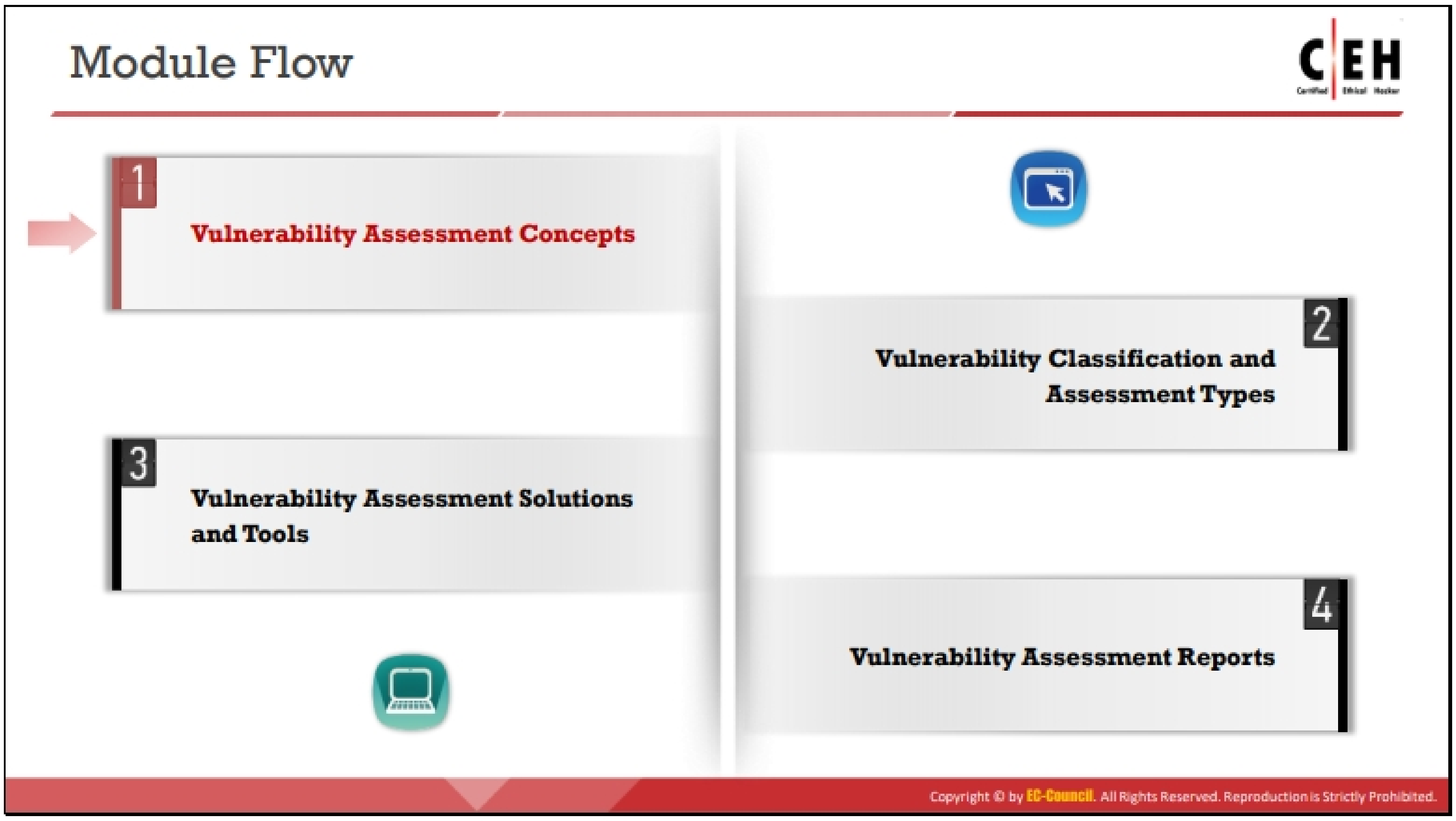
Attackers perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by attackers to further exploit that target network.

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute a vulnerability assessment.

This module starts with an introduction to vulnerability assessment concepts. It also discusses the various vulnerability scoring systems, vulnerability databases, vulnerability management life cycle, and various approaches and tools used to perform vulnerability assessments. This module will provide knowledge about the tools and techniques used by attackers to perform a quality vulnerability analysis. It concludes with an analysis of the vulnerability assessment reports that help an ethical hacker to fix the identified vulnerabilities.

At the end of this module, you will be able to:

- Understand vulnerability research, vulnerability assessment, and vulnerability scoring systems
- Describe the vulnerability management life cycle (vulnerability assessment phases)
- Understand various types of vulnerabilities and vulnerability assessment techniques
- Understand different approaches to vulnerability assessment solutions
- Describe different characteristics of good vulnerability assessment solutions
- Explain different types of vulnerability assessment tools and the criteria for choosing them
- Use various vulnerability assessment tools
- Generate and analyze vulnerability assessment reports



Module Flow

1 **Vulnerability Assessment Concepts**

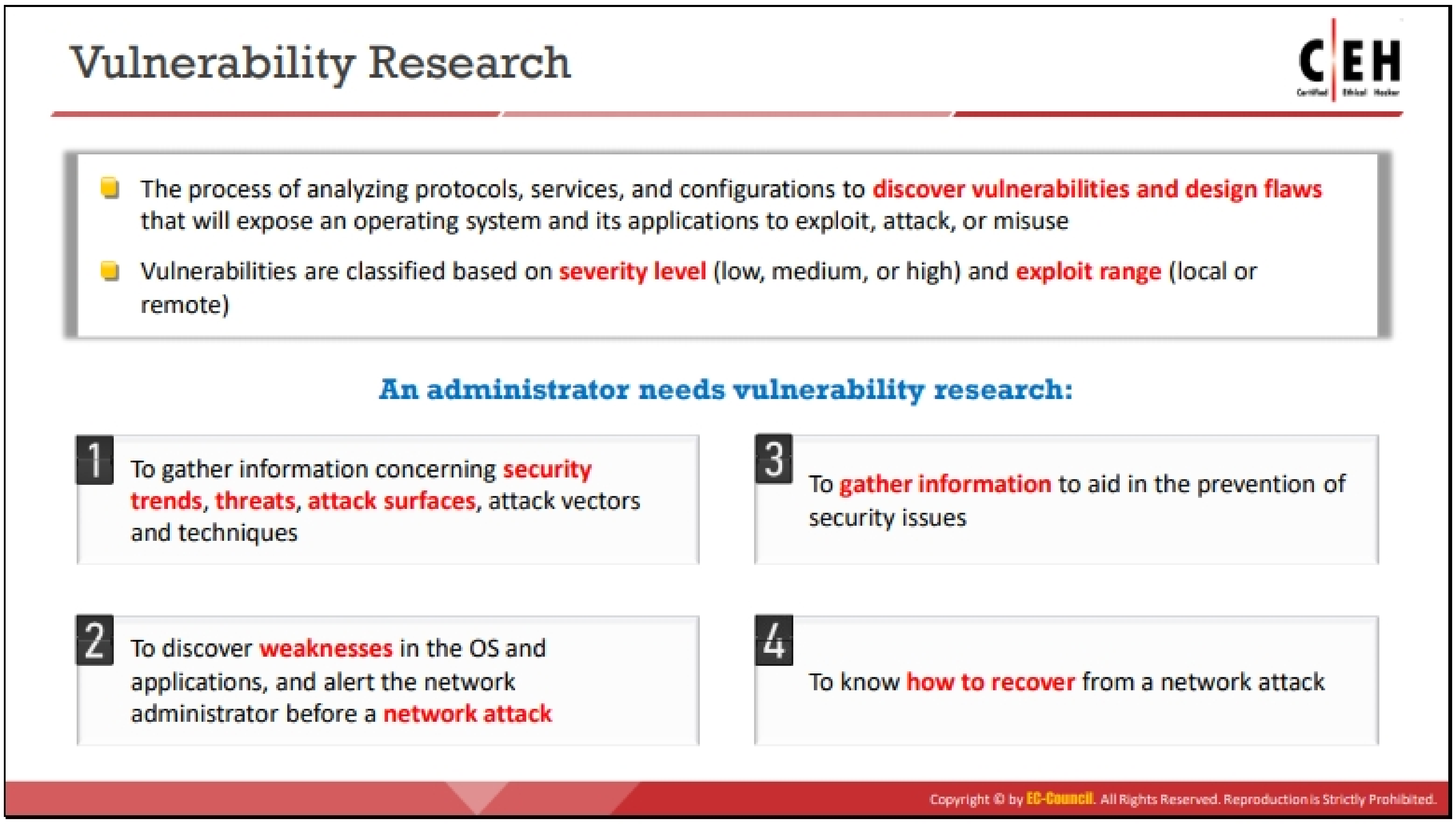
2 **Vulnerability Classification and Assessment Types**

3 **Vulnerability Assessment Solutions and Tools**

4 **Vulnerability Assessment Reports**

Vulnerability Assessment Concepts

There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources. This section gives an overview of vulnerability assessment, vulnerability scoring systems, vulnerability databases, and the vulnerability assessment life cycle.



Vulnerability Research

- The process of analyzing protocols, services, and configurations to **discover vulnerabilities and design flaws** that will expose an operating system and its applications to exploit, attack, or misuse
- Vulnerabilities are classified based on **severity level** (low, medium, or high) and **exploit range** (local or remote)

An administrator needs vulnerability research:

1. To gather information concerning **security trends**, **threats**, **attack surfaces**, attack vectors and techniques
2. To discover **weaknesses** in the OS and applications, and alert the network administrator before a **network attack**
3. To **gather information** to aid in the prevention of security issues
4. To know **how to recover** from a network attack

Vulnerability Research

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

An administrator needs vulnerability research:

- To gather information about security trends, newly discovered threats, attack surfaces, attack vectors and techniques
- To find weaknesses in the OS and applications and alert the network administrator before a network attack
- To understand information that helps prevent security problems
- To know how to recover from a network attack

An ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits to stay one step ahead of attackers through vulnerability research, which includes:

- Discovering the system design faults and weaknesses that might allow attackers to compromise a system
- Staying updated about new products and technologies and reading news related to current exploits
- Checking underground hacking web sites (Deep and Dark websites) for newly discovered vulnerabilities and exploits
- Checking newly released alerts regarding relevant innovations and product improvements for security systems

Security experts and vulnerability scanners classify vulnerabilities by:

- Severity level (low, medium, or high)
- Exploit range (local or remote)

Ethical hackers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to find vulnerabilities.

Resources for Vulnerability Research

Microsoft Vulnerability Research (MSVR)
https://www.microsoft.com

Dark Reading
https://www.darkreading.com

SecurityTracker
https://securitytracker.com

Trend Micro
https://www.trendmicro.com

Security Magazine
https://www.securitymagazine.com

PenTest Magazine
https://pentestmag.com

SC Magazine
https://www.scmagazine.com

Exploit Database
https://www.exploit-db.com

SecurityFocus
https://www.securityfocus.com

Help Net Security
https://www.helpnetsecurity.com

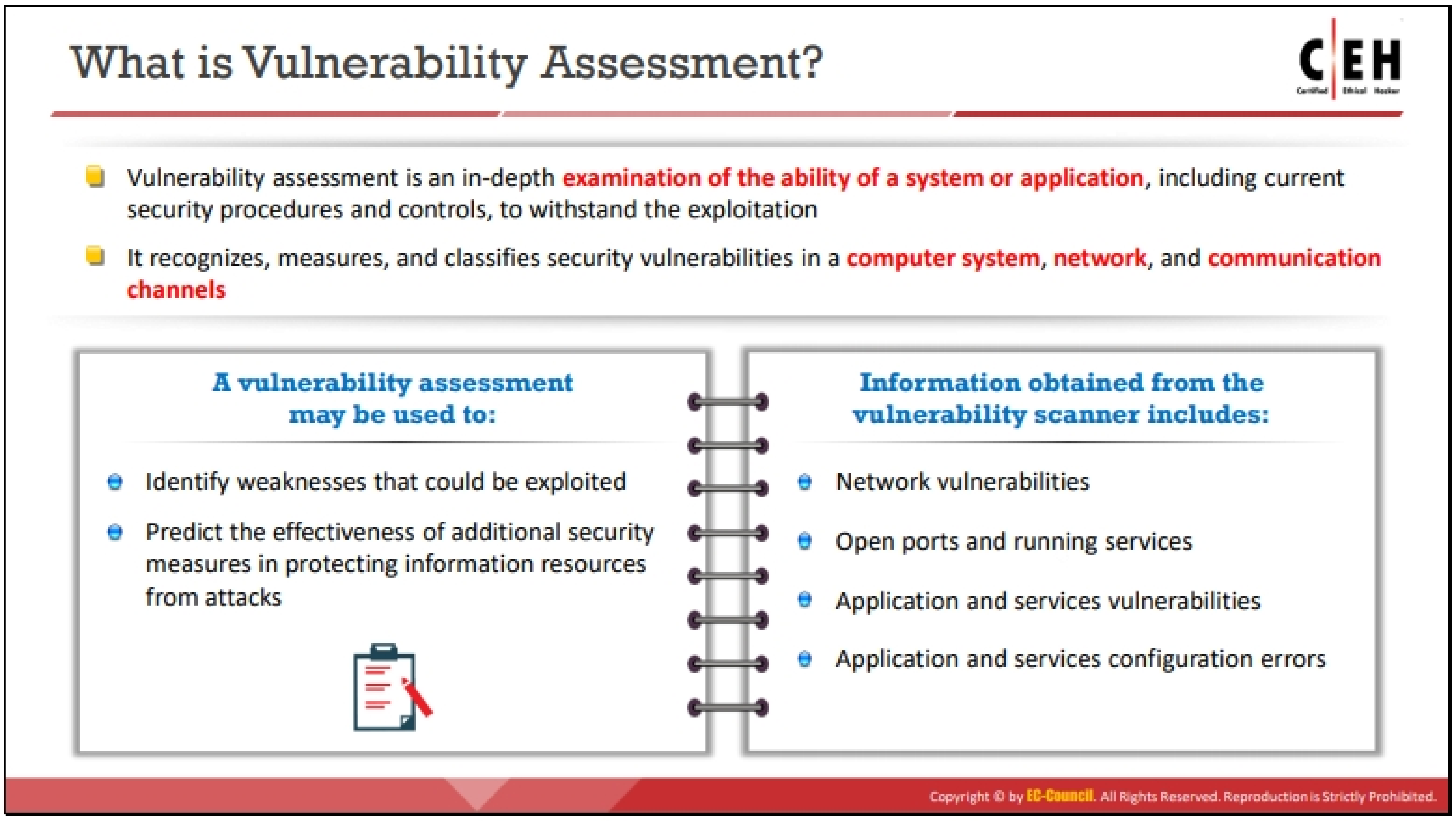
HackerStorm
http://www.hackerstorm.co.uk

Computerworld
https://www.computerworld.com

Resources for Vulnerability Research

The following are some of the online websites used to perform vulnerability research:

- Microsoft Vulnerability Research (MSVR) (*https://www.microsoft.com*)
- Dark Reading (*https://www.darkreading.com*)
- SecurityTracker (*https://securitytracker.com*)
- Trend Micro (*https://www.trendmicro.com*)
- Security Magazine (*https://www.securitymagazine.com*)
- PenTest Magazine (*https://pentestmag.com*)
- SC Magazine (*https://www.scmagazine.com*)
- Exploit Database (*https://www.exploit-db.com*)
- SecurityFocus (*https://www.securityfocus.com*)
- Help Net Security (*https://www.helpnetsecurity.com*)
- HackerStorm (*http://www.hackerstorm.co.uk*)
- Computerworld (*https://www.computerworld.com*)
- WindowsSecurity (*http://www.windowsecurity.com*)
- D'Crypt (*https://www.d-crypt.com*)



What is Vulnerability Assessment?

- Vulnerability assessment is an in-depth **examination of the ability of a system or application**, including current security procedures and controls, to withstand the exploitation
- It recognizes, measures, and classifies security vulnerabilities in a **computer system**, **network**, and **communication channels**

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attacks

Information obtained from the vulnerability scanner includes:

- Network vulnerabilities
- Open ports and running services
- Application and services vulnerabilities
- Application and services configuration errors

What is Vulnerability Assessment?

A vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system. Additionally, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attack

Typically, vulnerability-scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities. Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers

- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Errors in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities
- EOL/EOS software information
- Missing patches and hotfixes
- Weak network configurations and misconfigured or risky ports
- Help to verify the inventory of all devices on the network

There are two approaches to network vulnerability scanning:

- **Active Scanning**: The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

  Example: An attacker sends probes and specially crafted requests to the target host in the network to identify vulnerabilities.

- **Passive Scanning**: The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weaknesses but does not provide a path for directly combating attacks.

  Example: An attacker guesses the operating system information, applications, and application and service versions by observing the TCP connection setup and teardown.

Attackers scan for vulnerabilities using tools such as Nessus, Qualys, GFI LanGuard, and OpenVAS. Vulnerability scanning enables an attacker to identify network vulnerabilities, open ports and running services, application and services configuration errors, and application and service vulnerabilities.

Limitations of Vulnerability Assessment

The following are some of the limitations of vulnerability assessments:

- Vulnerability-scanning software is limited in its ability to detect vulnerabilities at a given point in time
- Vulnerability-scanning software must be updated when new vulnerabilities are discovered or when improvements are made to the software being used
- Software is only as effective as the maintenance performed on it by the software vendor and by the administrator who uses it
- Vulnerability Assessment does not measure the strength of security controls

- Vulnerability-scanning software itself is not immune to software engineering flaws that might lead to it missing serious vulnerabilities
- Human judgment is needed to analyze the data after scanning and identifying the false positives and false negatives.

The methodology used might have an impact on the test results. For example, vulnerability-scanning software that runs under the security context of the domain administrator will yield different results than software that runs under the security context of an authenticated or non-authenticated user. Similarly, diverse vulnerability-scanning software packages assess security differently and have unique features. This can influence the assessment results.

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)

- CVSS provides an open framework **for communicating the characteristics and impacts** of IT vulnerabilities
- Its quantitative model ensures repeatable accurate measurement, while enabling users to view the **underlying vulnerability characteristics** used to **generate the scores**

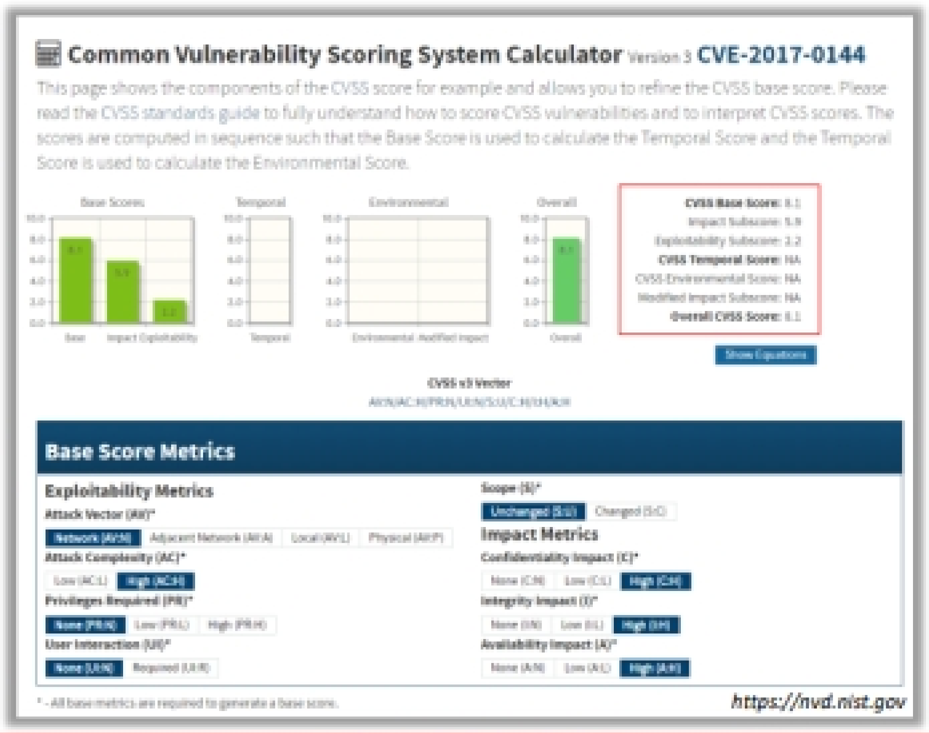
CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

https://www.first.org



Common Vulnerability Scoring System Calculator Version 3 **CVE-2017-0144**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 8.1
Impact Subscore: 5.9
Exploitability Subscore: 2.2
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.1

CVSS v3 Vector
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics
Attack Vector (AV)*: Network (AV:N)
Attack Complexity (AC)*: High (AC:H)
Privileges Required (PR)*: None (PR:N)
User Interaction (UI)*: None (UI:N)
Scope (S)*: Unchanged (S:U)

Impact Metrics
Confidentiality Impact (C)*: High (C:H)
Integrity Impact (I)*: High (I:H)
Availability Impact (A)*: High (A:H)

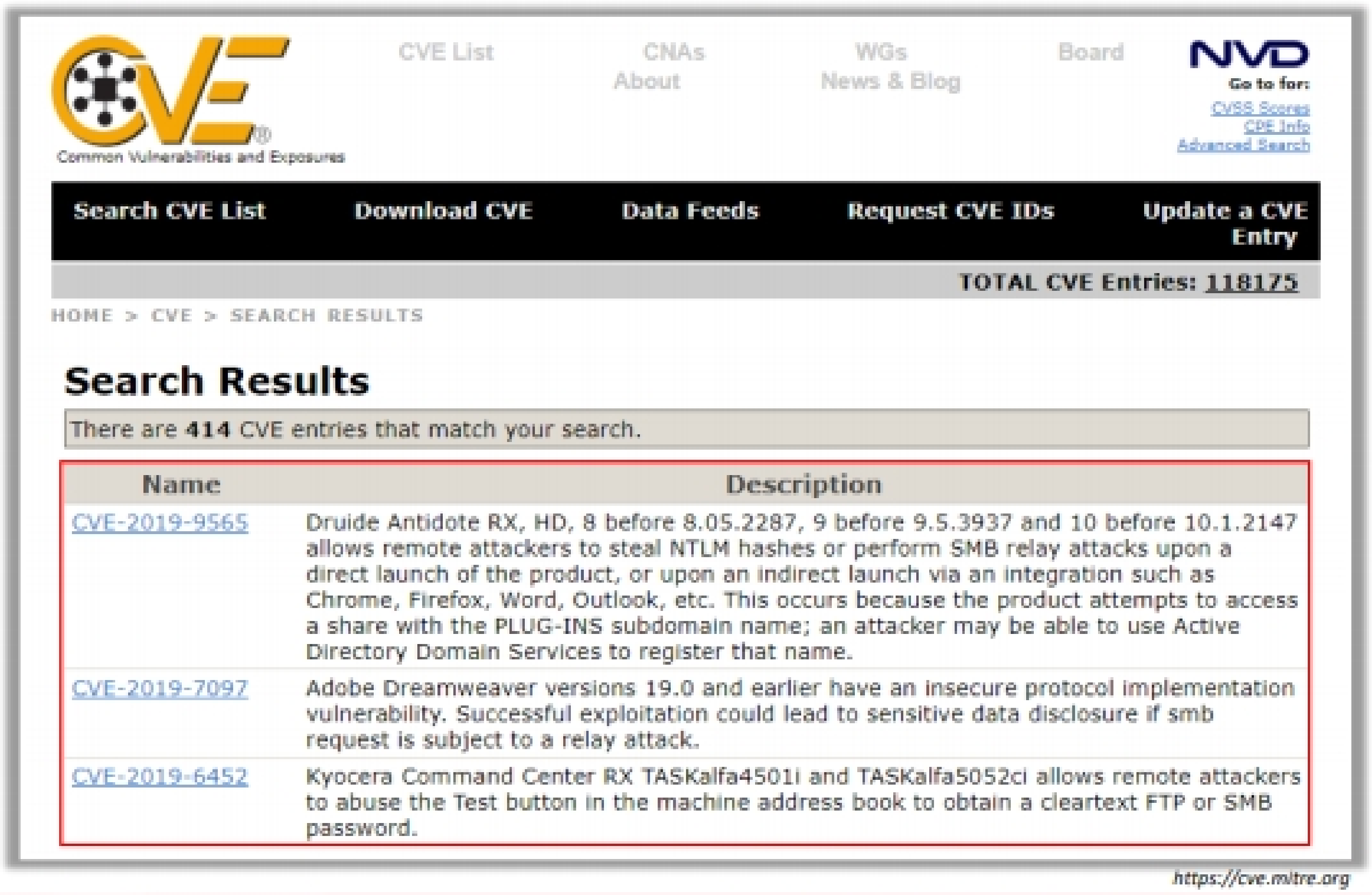
* - All base metrics are required to generate a base score.

https://nvd.nist.gov

Vulnerability Scoring Systems and Databases (Cont'd)

Common Vulnerabilities and Exposures (CVE)

A publicly available and free-to-use **list or dictionary of standardized identifiers** for common software vulnerabilities and exposures



TOTAL CVE Entries: 118175

HOME > CVE > SEARCH RESULTS

Search Results

There are **414** CVE entries that match your search.

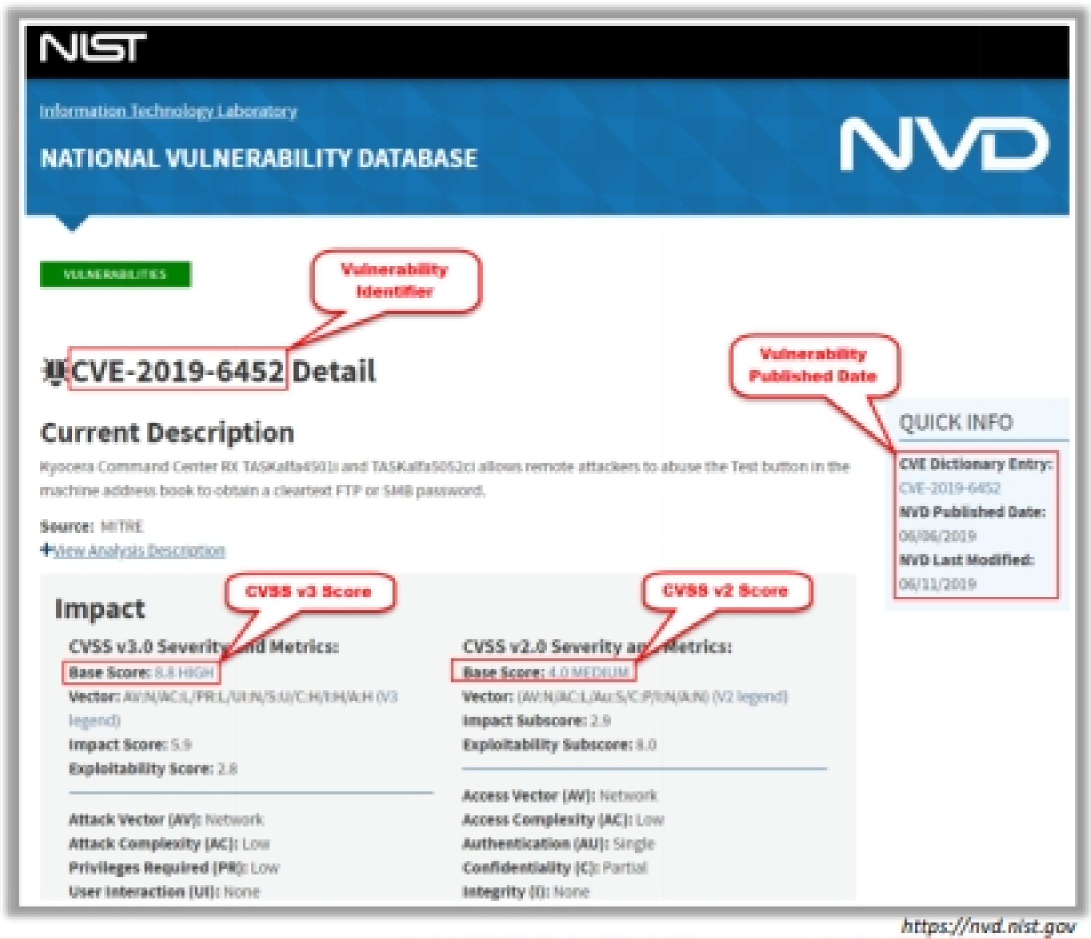
Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

https://cve.mitre.org

Vulnerability Scoring Systems and Databases (Cont'd)

National Vulnerability Database (NVD)

- A **U.S. government repository** of standards-based vulnerability management data represented using the **Security Content Automation Protocol** (SCAP)
- These data **enable the automation of vulnerability management**, security measurement, and compliance
- The NVD includes **databases of security checklist** references, security-related software flaws, misconfigurations, product names, and impact metrics


NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
Vulnerability Identifier
Vulnerability Published Date
CVSS v3 Score
CVSS v2 Score

CVE-2019-6452 Detail

Current Description

Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 2.8

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None

CVSS v2.0 Severity and Metrics:
Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): None

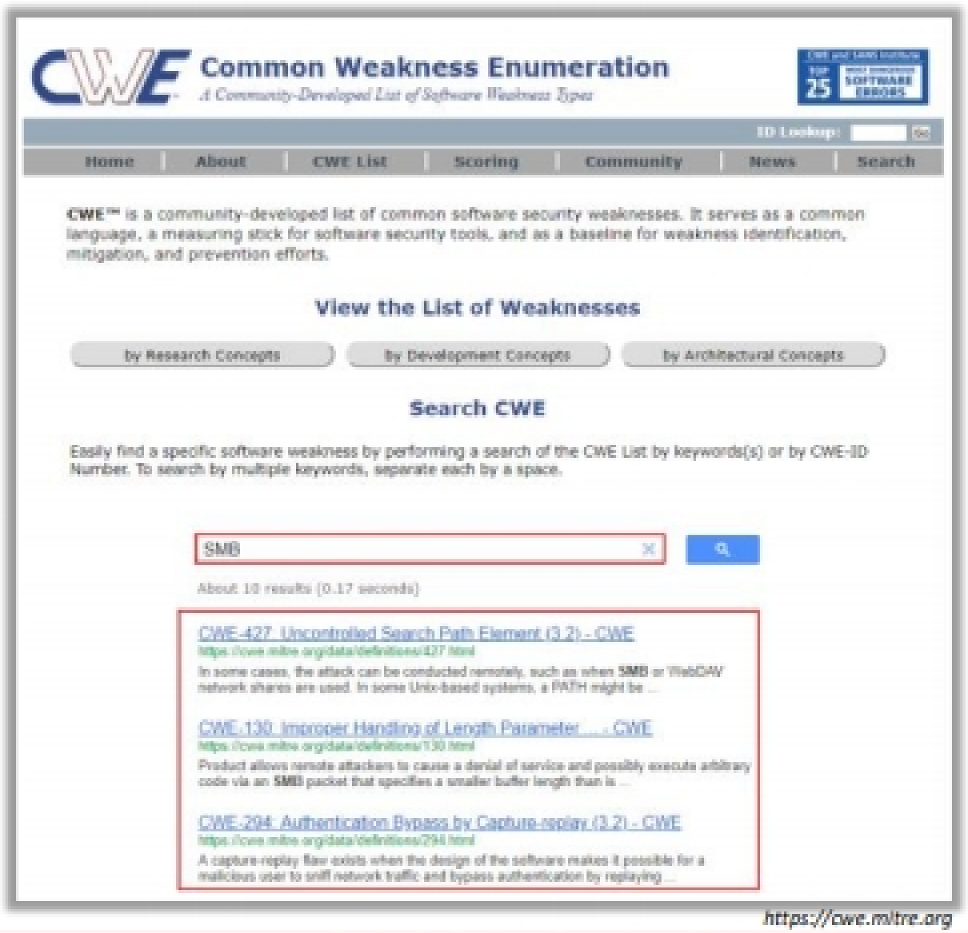
QUICK INFO
CVE Dictionary Entry: CVE-2019-6452
NVD Published Date: 06/06/2019
NVD Last Modified: 06/11/2019

https://nvd.nist.gov

Vulnerability Scoring Systems and Databases (Cont'd)

Common Weakness Enumeration (CWE)

- A **category system** for **software vulnerabilities and weaknesses**
- It is sponsored by the **National Cybersecurity FFRDC**, which is owned by **The MITRE Corporation**, with support from **US-CERT** and the **National Cyber Security Division** of the **U.S. Department of Homeland Security**
- It has over **600 categories** of weaknesses, which enable CWE to be effectively employed by the community as a **baseline for weakness identification**, **mitigation**, and **prevention efforts**


CWE
Common Weakness Enumeration
A Community-Developed List of Software Weakness Types
CWE and SANS Institute TOP 25 SOFTWARE ERRORS
ID Lookup:
Home
About
CWE List
Scoring
Community
News
Search
by Research Concepts
by Development Concepts
by Architectural Concepts

CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

Search CWE

Easily find a specific software weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

SMB

About 10 results (0.17 seconds)

CWE-427: Uncontrolled Search Path Element (3.2) - CWE
https://cwe.mitre.org/data/definitions/427.html
In some cases, the attack can be conducted remotely, such as when SMB or WebDAV network shares are used. In some Unix-based systems, a PATH might be ...

CWE-130: Improper Handling of Length Parameter ... - CWE
https://cwe.mitre.org/data/definitions/130.html
Product allows remote attackers to cause a denial of service and possibly execute arbitrary code via an SMB packet that specifies a smaller buffer length than is ...

CWE-294: Authentication Bypass by Capture-replay (3.2) - CWE
https://cwe.mitre.org/data/definitions/294.html
A capture-replay flaw exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying ...

https://cwe.mitre.org

Vulnerability Scoring Systems and Databases

Due to the growing severity of cyber-attacks, vulnerability research has become critical as it helps to mitigate the chance of attacks. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that can be exploited by attackers. Vulnerability scoring systems and vulnerability databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities. Vulnerability databases collect and maintain information about various vulnerabilities present in information systems.

Following are some of the vulnerability scoring systems and databases:

- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Weakness Enumeration (CWE)

Common Vulnerability Scoring System (CVSS)

Source: *https://www.first.org*, *https://nvd.nist.gov*

CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. The system's quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritizing vulnerability remediation activities and calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

CVSS helps capture the principal characteristics of a vulnerability and produce a numerical score to reflect its severity. This numerical score can thereafter be translated into a qualitative representation (such as low, medium, high, or critical) to help organizations properly assess and prioritize their vulnerability management processes.

CVSS assessment consists of three metrics for measuring vulnerabilities:

- **Base Metric**: Represents the inherent qualities of a vulnerability
- **Temporal Metric**: Represents the features that continue to change during the lifetime of the vulnerability.
- **Environmental Metric:** Represents vulnerabilities that are based on a particular environment or implementation.

Each metric sets a score from 1–10, with 10 being the most severe. The CVSS score is calculated and generated by a vector string, which represents the numerical score for each group in the form of a block of text. The CVSS calculator ranks the security vulnerabilities and provides the user with information on the overall severity and risk related to the vulnerability.

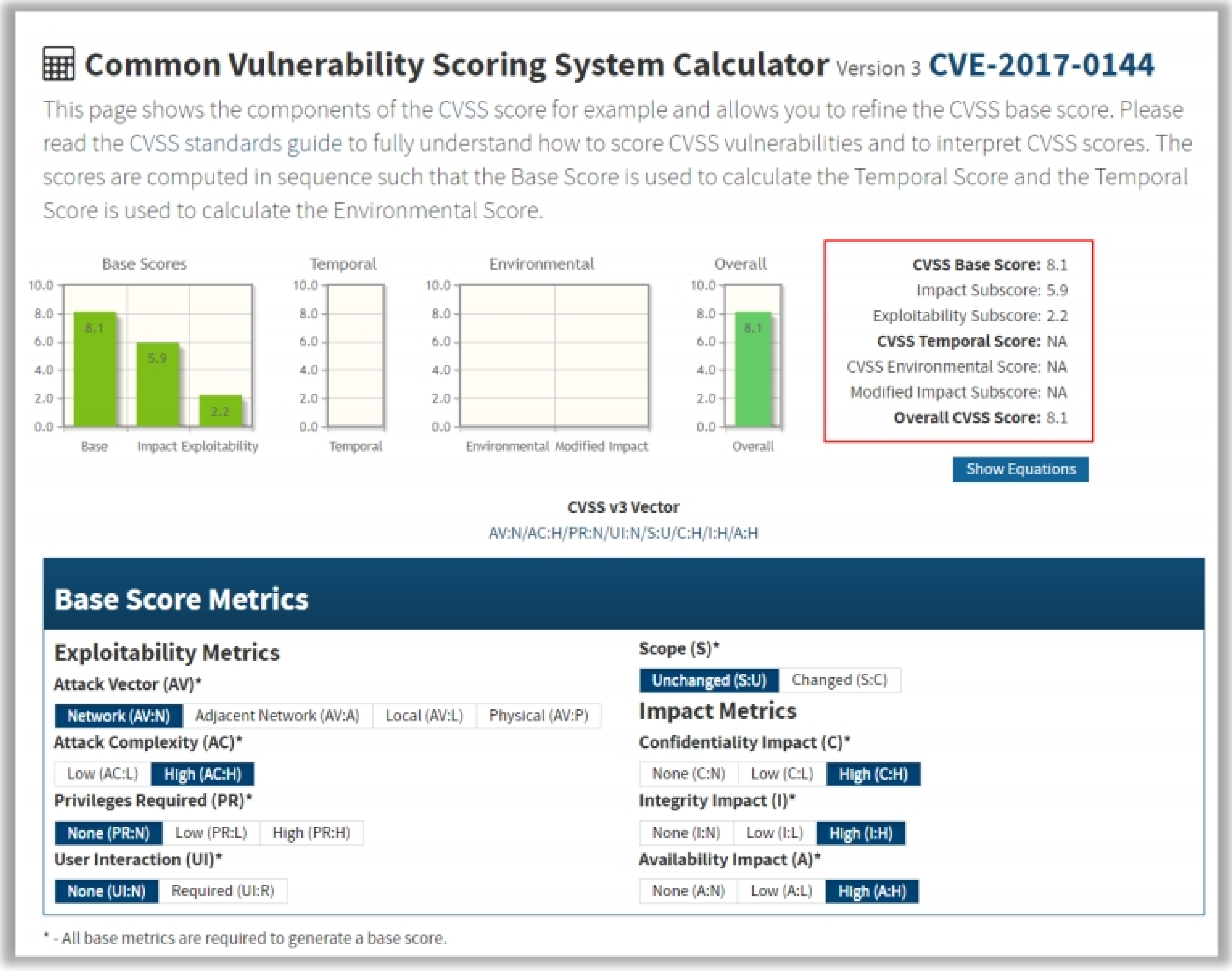
Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9

High	7.0-8.9
Critical	9.0-10.0

Table 5.1: CVSS v3.0 ratings

Severity	**Base Score Range**
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Table 5.2: CVSS v2.0 ratings



Common Vulnerability Scoring System Calculator Version 3 **CVE-2017-0144**

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 8.1
Impact Subscore: 5.9
Exploitability Subscore: 2.2
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.1

CVSS v3 Vector
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*: Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*: Low (AC:L) | High (AC:H)

Privileges Required (PR)*: None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*: None (UI:N) | Required (UI:R)

Scope (S)*: Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*: None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*: None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*: None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

Figure 5.1: Common Vulnerability Scoring System Calculator Version 3

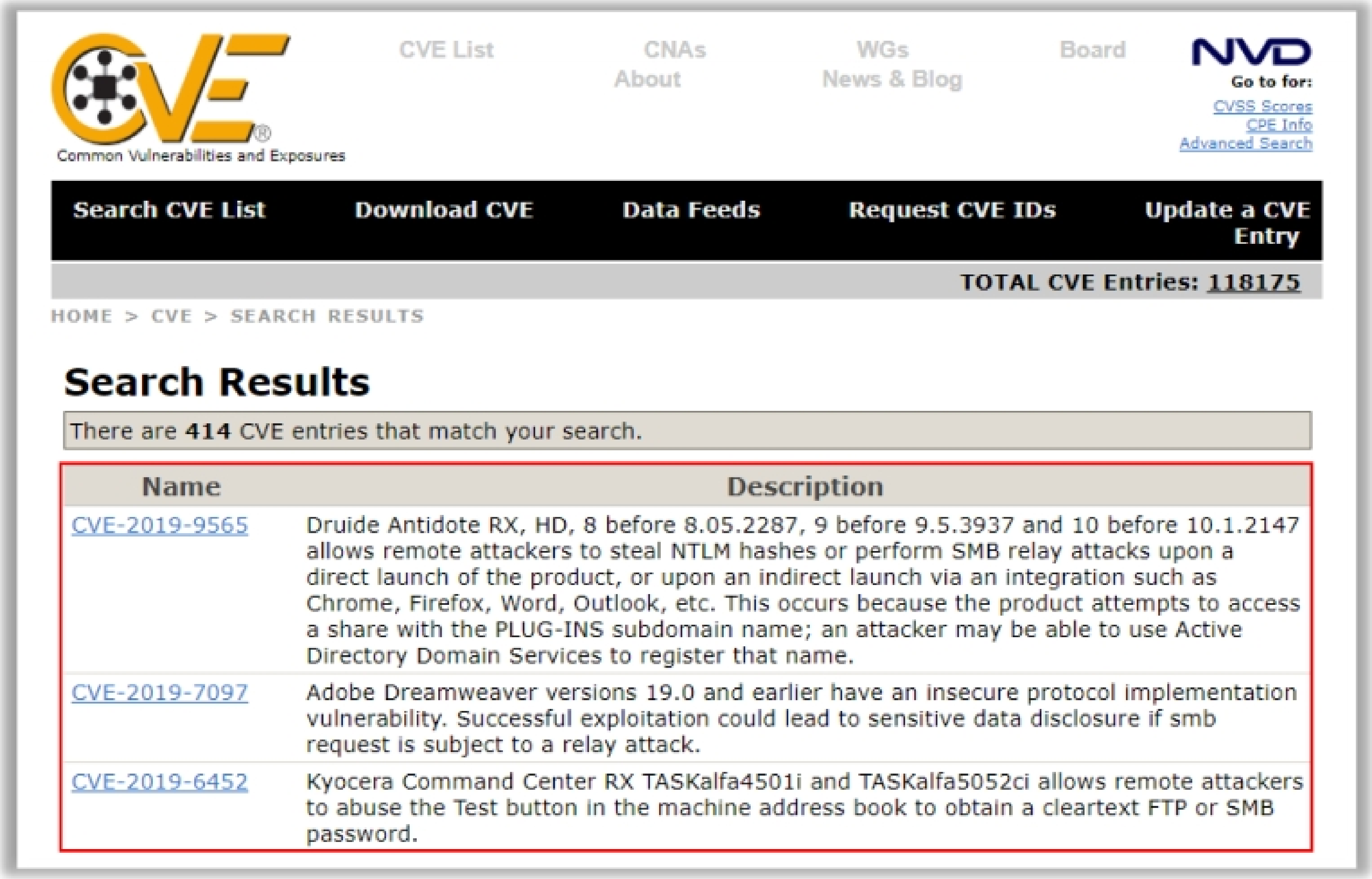
Common Vulnerabilities and Exposures (CVE)

Source: *https://cve.mitre.org*

CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. The use of CVE Identifiers, or "CVE IDs," which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when discussing or sharing information about a unique software or firmware vulnerability. CVE provides a baseline for tool evaluation and enables data exchange for cybersecurity automation. CVE IDs provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

What CVE is:

- One identifier for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- A method for disparate databases and tools to "speak" the same language
- The way to interoperability and better security coverage
- A basis for evaluation among services, tools, and databases
- Free for the public to download and use
- Industry-endorsed via the CVE Numbering Authorities, CVE Board, and the numerous products and services that include CVE



TOTAL CVE Entries: 118175

HOME > CVE > SEARCH RESULTS

Search Results

There are **414** CVE entries that match your search.

Name	Description
CVE-2019-9565	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.
CVE-2019-7097	Adobe Dreamweaver versions 19.0 and earlier have an insecure protocol implementation vulnerability. Successful exploitation could lead to sensitive data disclosure if smb request is subject to a relay attack.
CVE-2019-6452	Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

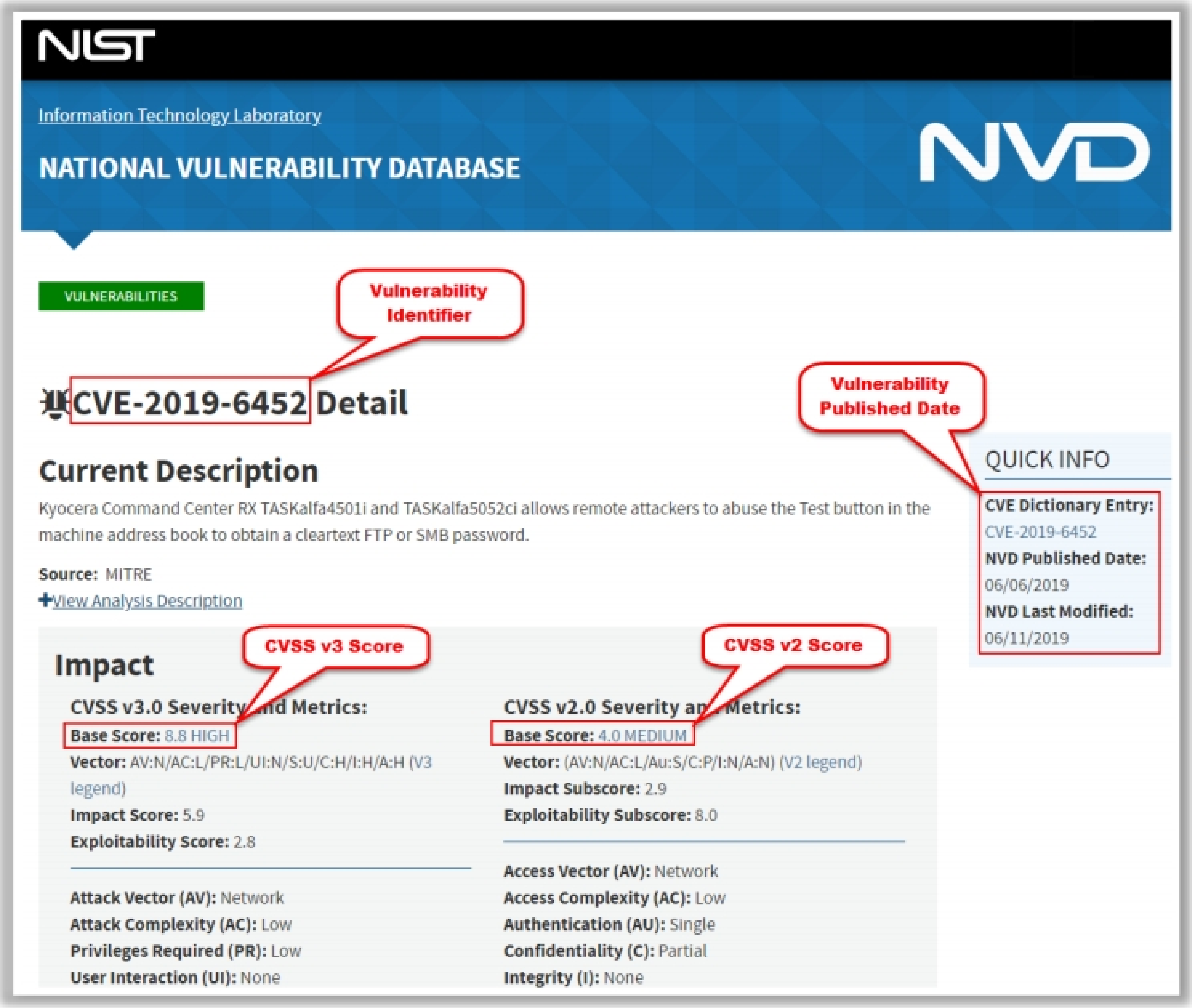
Figure 5.2: Common Vulnerabilities and Exposures (CVE)

National Vulnerability Database (NVD)

Source: *https://nvd.nist.gov*

The NVD is the U.S. government repository of standards-based vulnerability management data. It uses the Security Content Automation Protocol (SCAP). Such data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

The NVD performs an analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with the analysis of CVEs by aggregating data points from the description, references supplied, and any supplemental data that are publicly available. This analysis results in association impact metrics (Common Vulnerability Scoring System – CVSS), vulnerability types (Common Weakness Enumeration — CWE), and applicability statements (Common Platform Enumeration — CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing; it relies on vendors, third party security researchers, and vulnerability coordinators to provide information that is used to assign these attributes.


NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITIES
Vulnerability Identifier
Vulnerability Published Date
CVSS v3 Score
CVSS v2 Score

CVE-2019-6452 Detail

Current Description

Kyocera Command Center RX TASKalfa4501i and TASKalfa5052ci allows remote attackers to abuse the Test button in the machine address book to obtain a cleartext FTP or SMB password.

Source: MITRE

+View Analysis Description

QUICK INFO

CVE Dictionary Entry: CVE-2019-6452
NVD Published Date: 06/06/2019
NVD Last Modified: 06/11/2019

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 2.8

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None

CVSS v2.0 Severity and Metrics:

Base Score: 4.0 MEDIUM
Vector: (AV:N/AC:L/Au:S/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 8.0

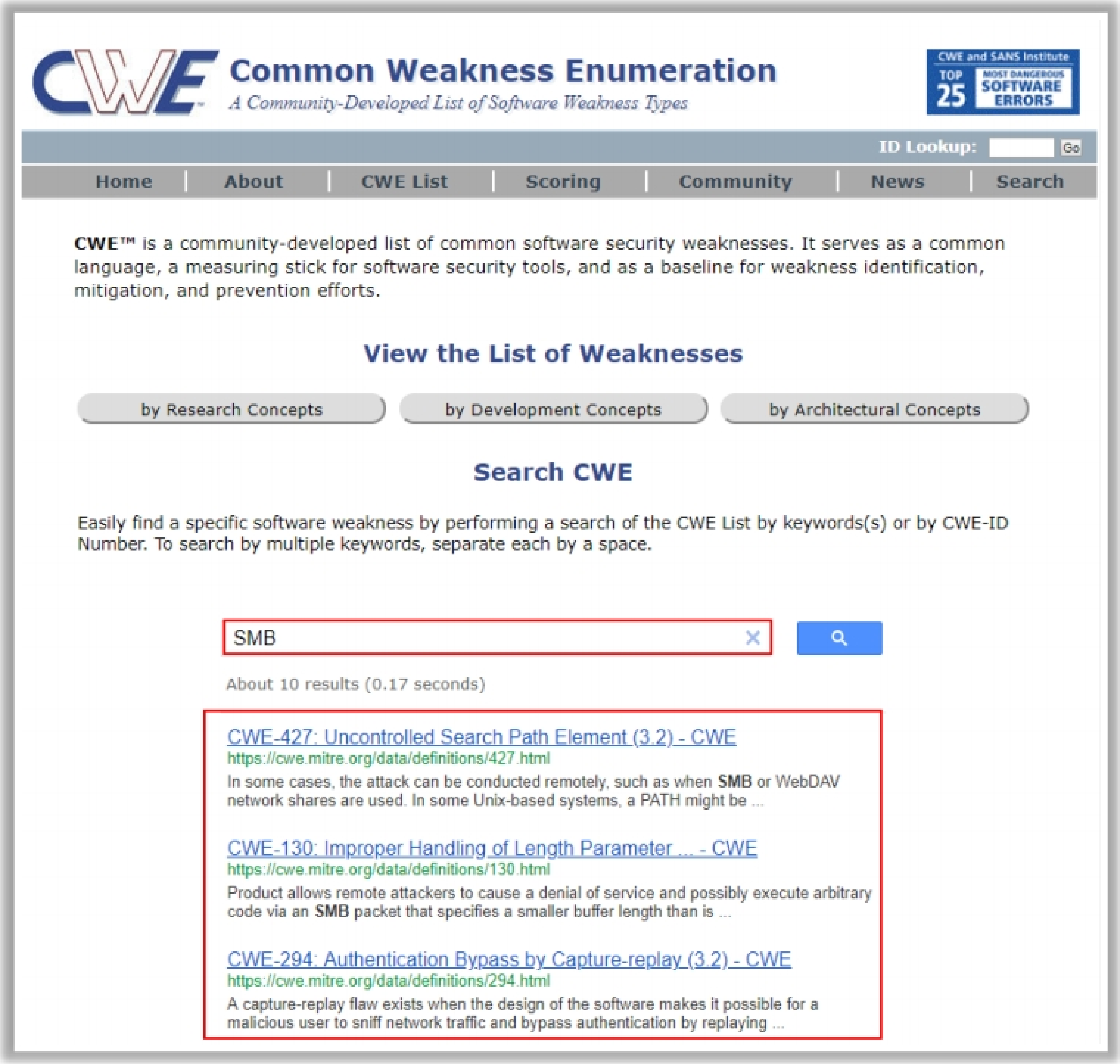
Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): Single
Confidentiality (C): Partial
Integrity (I): None

Figure 5.3: Screenshot showing CVE details in the National Vulnerability Database (NVD)

Common Weakness Enumeration (CWE)

Source: *https://cwe.mitre.org*

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security. The latest version 3.2 of the CWE standard was released in January 2019. It has over 600 categories of weaknesses, which gives CWE the ability to be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. It also has an advanced search technique where attackers can search and view weaknesses based on research concepts, development concepts, and architectural concepts.


CWE
Common Weakness Enumeration
A Community-Developed List of Software Weakness Types
CWE and SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS
ID Lookup:
Go
Home
About
CWE List
Scoring
Community
News
Search

CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

by Research Concepts
by Development Concepts
by Architectural Concepts

Search CWE

Easily find a specific software weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

SMB

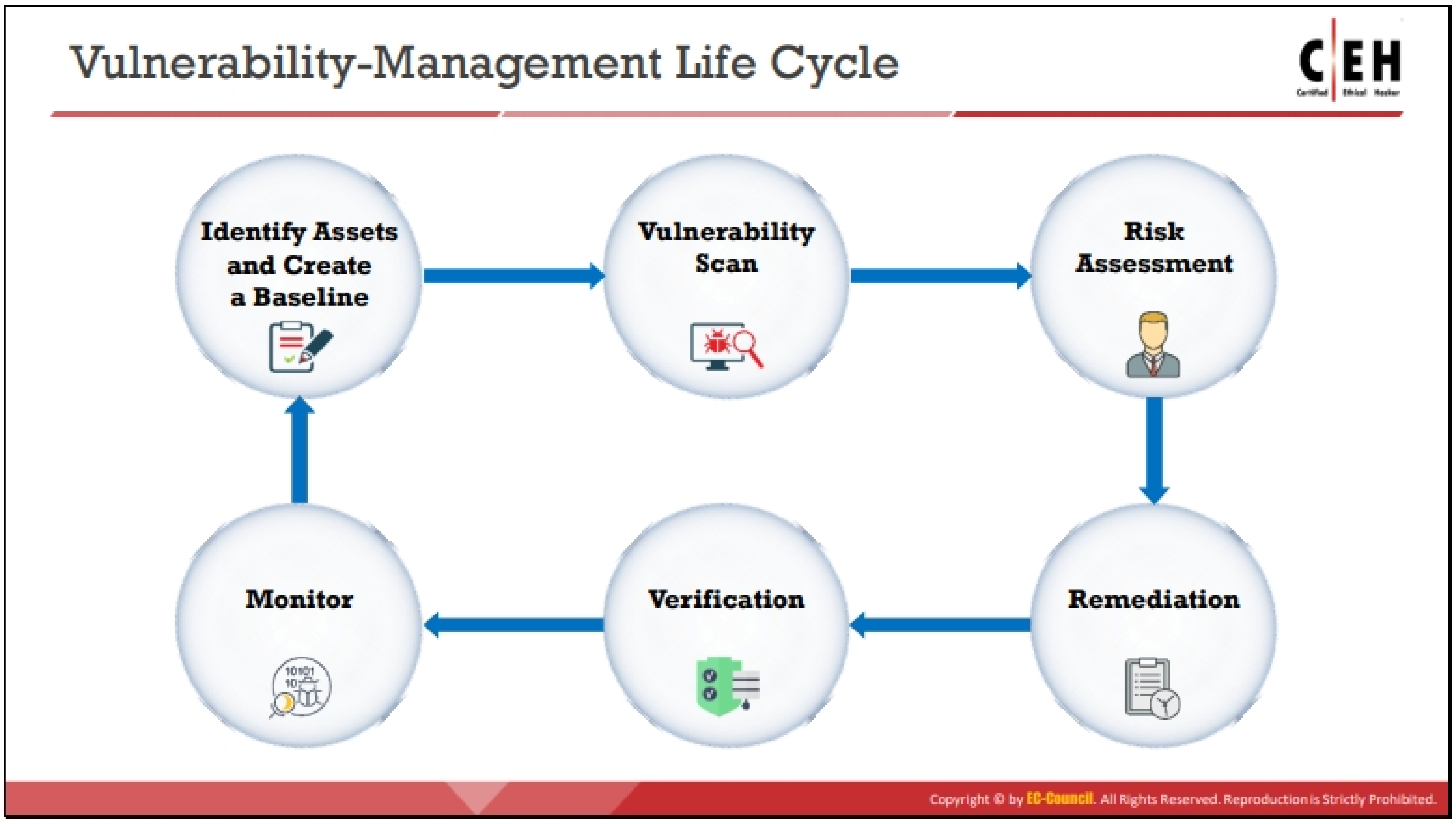
About 10 results (0.17 seconds)

CWE-427: Uncontrolled Search Path Element (3.2) - CWE
https://cwe.mitre.org/data/definitions/427.html
In some cases, the attack can be conducted remotely, such as when **SMB** or WebDAV network shares are used. In some Unix-based systems, a PATH might be ...

CWE-130: Improper Handling of Length Parameter ... - CWE
https://cwe.mitre.org/data/definitions/130.html
Product allows remote attackers to cause a denial of service and possibly execute arbitrary code via an **SMB** packet that specifies a smaller buffer length than is ...

CWE-294: Authentication Bypass by Capture-replay (3.2) - CWE
https://cwe.mitre.org/data/definitions/294.html
A capture-replay flaw exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying ...

Figure 5.4: Screenshot showing CWE results for SMB query



Vulnerability-Management Life Cycle

Identify Assets and Create a Baseline

Vulnerability Scan

Risk Assessment

Remediation

Verification

Monitor

Vulnerability-Management Life Cycle

The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are identified. The implementation of a vulnerability management lifecycle helps gain a strategic perspective regarding possible cybersecurity threats and renders insecure computing environments more resilient to attacks.

Vulnerability management should be implemented in every organization as it evaluates and controls the risks and vulnerabilities in the system. The management process continuously examines the IT environments for vulnerabilities and risks associated with the system.

Organizations should maintain a proper vulnerability management program to ensure overall information security. Vulnerability management provides the best results when it is implemented in a sequence of well-organized phases.

The phases involved in vulnerability management are:

- **Identify Assets and Create a Baseline**

  This phase identifies critical assets and prioritizes them to define the risk based on the criticality and value of each system. This creates a good baseline for vulnerability management. This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration of each system in order to develop and maintain a system baseline.

- **Vulnerability Scan**

  This phase is very crucial in vulnerability management. In this step, the security analyst performs the vulnerability scan on the network to identify the known vulnerabilities in the organization's infrastructure. Vulnerability scans can also be performed on applicable compliance templates to assess the organization's Infrastructure weaknesses against the respective compliance guidelines.

- **Risk Assessment**

  In this phase, all serious uncertainties that are associated with the system are assessed and prioritized, and remediation is planned to permanently eliminate system flaws. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. Remediation is planned based on the determined risk level. For example, vulnerabilities ranked high-risk are targeted first to decrease the chances of exploitation that would adversely impact the organization.

- **Remediation**

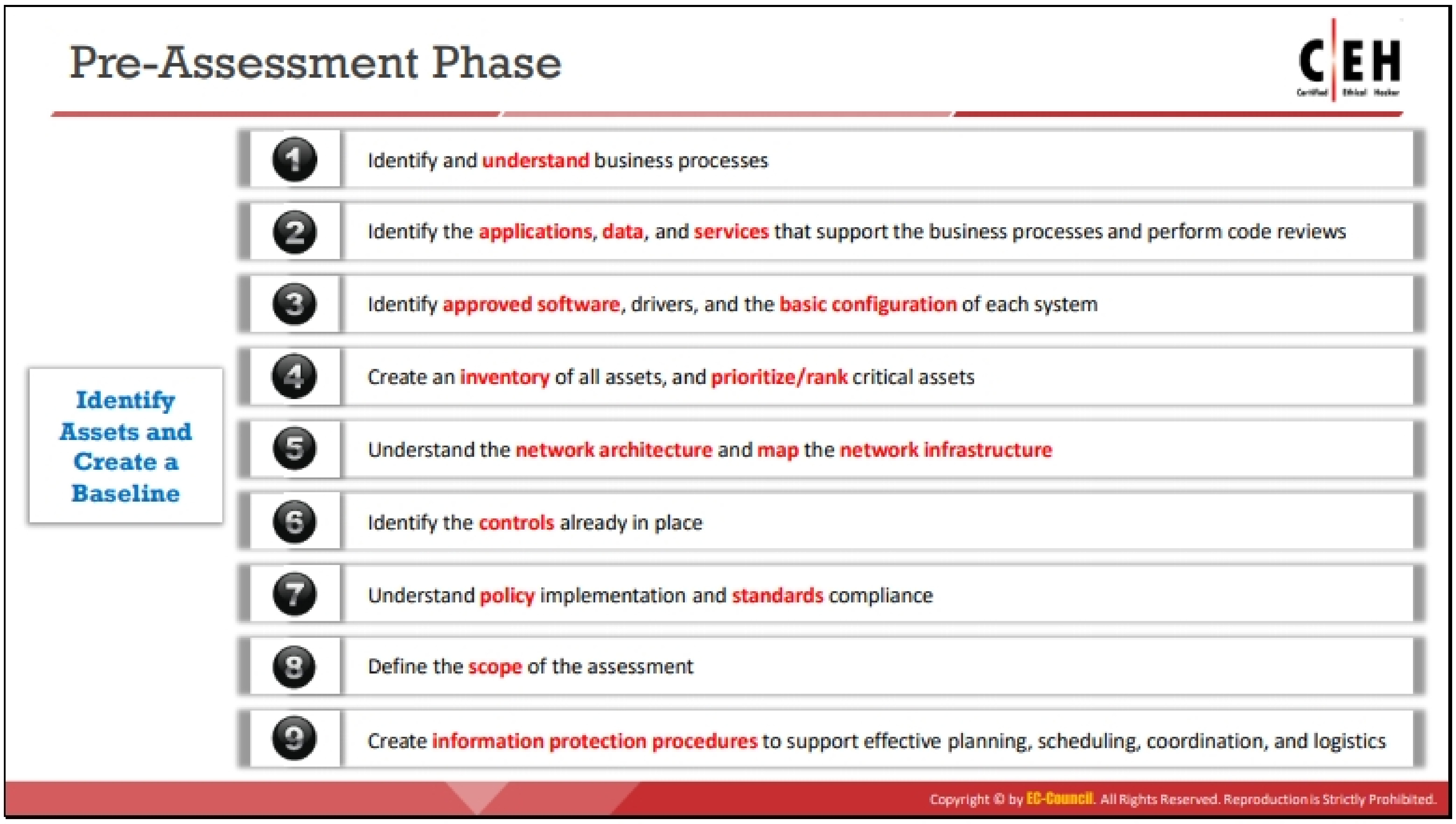
  Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

- **Verification**

  In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets. This phase provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not. Verification can be performed by using various means such as ticketing systems, scanners, and reports.

- **Monitor**

  Organizations need to performed regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved. As per security best practices, all phases of vulnerability management must be performed regularly.



Pre-Assessment Phase

Identify Assets and Create a Baseline

1. Identify and **understand** business processes
2. Identify the **applications**, **data**, and **services** that support the business processes and perform code reviews
3. Identify **approved software**, drivers, and the **basic configuration** of each system
4. Create an **inventory** of all assets, and **prioritize/rank** critical assets
5. Understand the **network architecture** and **map** the **network infrastructure**
6. Identify the **controls** already in place
7. Understand **policy** implementation and **standards** compliance
8. Define the **scope** of the assessment
9. Create **information protection procedures** to support effective planning, scheduling, coordination, and logistics

Pre-Assessment Phase

Identify Assets and Create a Baseline

The pre-assessment phase is a preparatory phase, which involves defining policies and standards, clarifying the scope of the assessment, designing appropriate information protection procedures, and identifying and prioritizing critical assets to create a good baseline for vulnerability management.

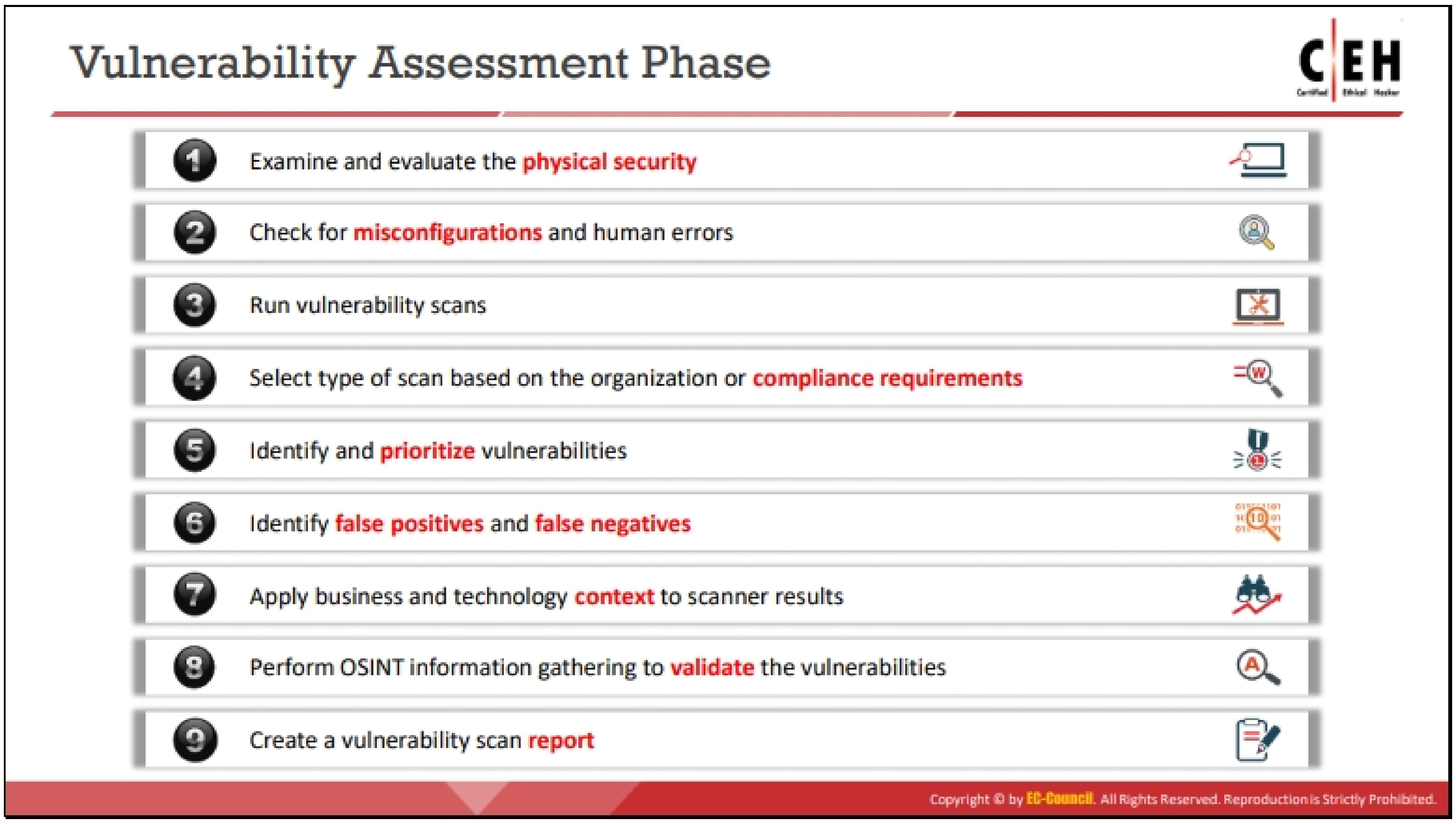
The following are the steps involved in creating a baseline:

1. Identify and understand business processes
2. Identify the applications, data, and services that support the business processes and perform code reviews
3. Identify the approved software, drivers, and basic configuration of each system
4. Create an inventory of all assets, and prioritize or rank the critical assets
5. Understand the network architecture and map the network infrastructure
6. Identify the controls already in place
7. Understand policy implementation and practice standard compliance with business processes
8. Define the scope of the assessment
9. Create information protection procedures to support effective planning, scheduling, coordination, and logistics

Classify the identified assets according to the business needs. Classification helps to identify the high business risks in an organization. Prioritize the rated assets based on the impact of their failure and their reliability in the business.

Prioritization helps:

- Evaluate and decide a solution for the consequence of the assets failing
- Examine the risk tolerance level
- Organize methods for prioritizing the assets



Vulnerability Assessment Phase

1. Examine and evaluate the **physical security**
2. Check for **misconfigurations** and human errors
3. Run vulnerability scans
4. Select type of scan based on the organization or **compliance requirements**
5. Identify and **prioritize** vulnerabilities
6. Identify **false positives** and **false negatives**
7. Apply business and technology **context** to scanner results
8. Perform OSINT information gathering to **validate** the vulnerabilities
9. Create a vulnerability scan **report**

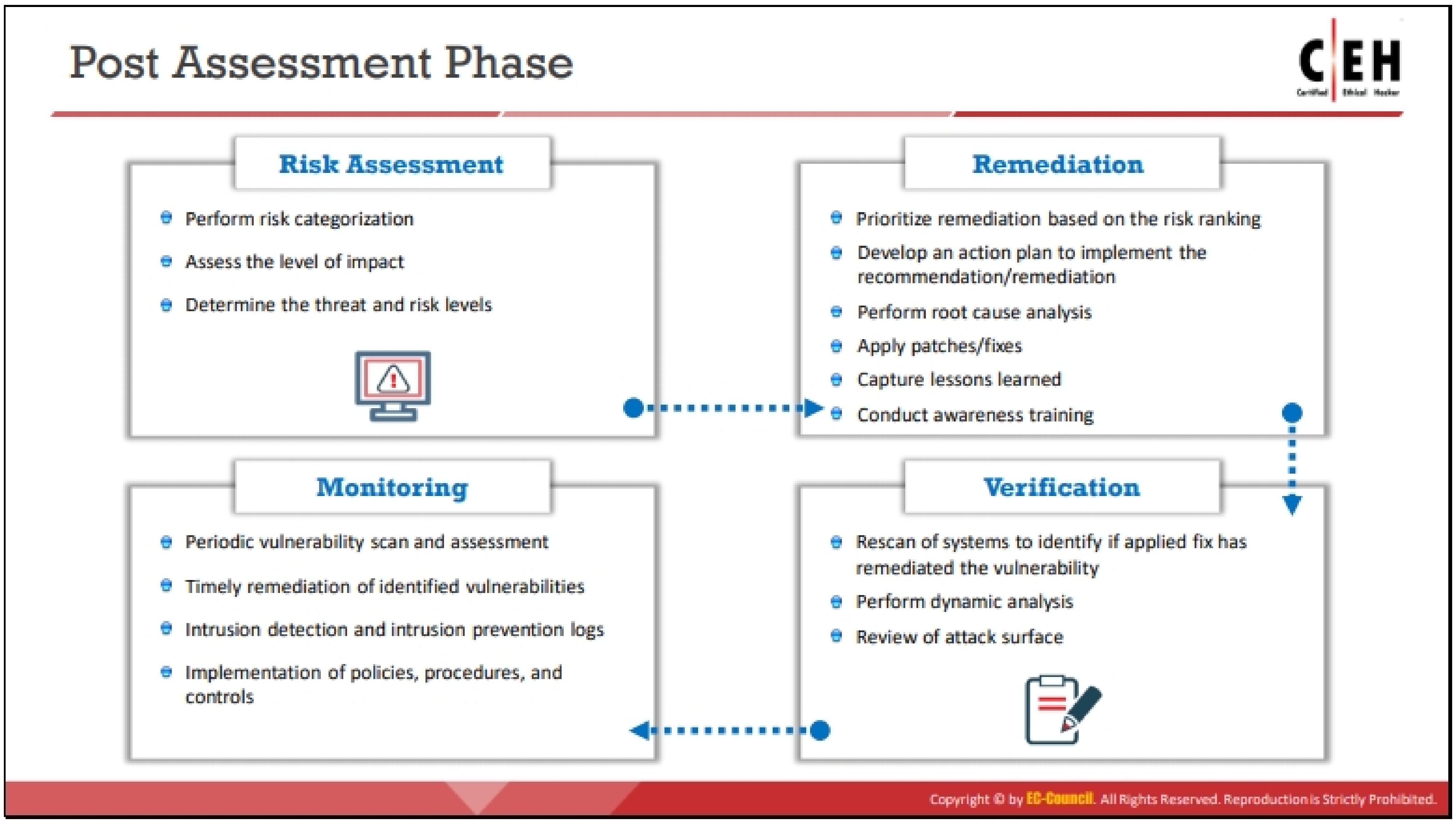
Vulnerability Assessment Phase

The vulnerability assessment phase refers to identifying vulnerabilities in the organization’s infrastructure, including the operating system, web applications, and web server. It helps identify the category and criticality of the vulnerability in an organization and minimizes the level of risk. The ultimate goal of vulnerability scanning is to scan, examine, evaluate, and report the vulnerabilities in the organization’s information system.

The assessment phase involves examining the architecture of the network, evaluating threats to the environment, performing penetration testing, examining and evaluating physical security, analyzing physical assets, assessing operational security, observing policies and procedures, and assessing the infrastructure’s interdependencies.

Steps involved in the assessment phase:

1. Examine and evaluate the physical security
2. Check for misconfigurations and human errors
3. Run vulnerability scans using tools
4. Select the type of scan based on the organization or compliance requirements
5. Identify and prioritize vulnerabilities
6. Identify false positives and false negatives
7. Apply the business and technology context to scanner results
8. Perform OSINT information gathering to validate the vulnerabilities
9. Create a vulnerability scan report



Post Assessment Phase

Risk Assessment

- Perform risk categorization
- Assess the level of impact
- Determine the threat and risk levels

Remediation

- Prioritize remediation based on the risk ranking
- Develop an action plan to implement the recommendation/remediation
- Perform root cause analysis
- Apply patches/fixes
- Capture lessons learned
- Conduct awareness training

Verification

- Rescan of systems to identify if applied fix has remediated the vulnerability
- Perform dynamic analysis
- Review of attack surface

Monitoring

- Periodic vulnerability scan and assessment
- Timely remediation of identified vulnerabilities
- Intrusion detection and intrusion prevention logs
- Implementation of policies, procedures, and controls

Post Assessment Phase

The post-assessment phase, also known as the recommendation phase, is performed after and based on risk assessment. Risk characterization is categorized by key criteria, which helps prioritize the list of recommendations.

The tasks performed in the post-assessment phase include:

- Creating a priority list for assessment recommendations based on the impact analysis
- Developing an action plan to implement the proposed remediation
- Capturing lessons learned to improve the complete process in the future
- Conducting training for employees

Post assessment includes risk assessment, remediation, verification, and monitoring.

- **Risk Assessment**

  In the risk assessment phase, risks are identified, characterized, and classified along with the techniques used to control or reduce their impact. It is an important step toward identifying the security weaknesses in the IT architecture of an organization.

  The tasks performed in the risk assessment phase include:

  - Perform risk categorization based on risk ranking (for example, critical, high, medium, and low)
  - Assess the level of impact
  - Determine the threat and risk levels

- **Remediation**

  Remediation refers to the steps taken to mitigate the identified vulnerabilities. These include steps like evaluating vulnerabilities, locating risks, and designing responses for vulnerabilities. It is important for the remediation process to be specific, measurable, attainable, relevant, and time-bound.

  The tasks performed in the remediation phase include:

  - Prioritize remediation based on the risk ranking
  - Develop an action plan to implement the recommendation or remediation
  - Perform a root-cause analysis
  - Apply patches and fixes
  - Capture lessons learned
  - Conduct awareness training
  - Perform exception handling and risk acceptance for the vulnerabilities that cannot be remediated

- **Verification**

  The verification phase helps security analysts verify the applied fixes that remediate a vulnerability by re-scanning the systems. In this phase, security analysts also verify whether all previous phases have been perfectly implemented. This phase includes the verification of the remedies used to mitigate risks.

  The tasks performed in the verification phase include:

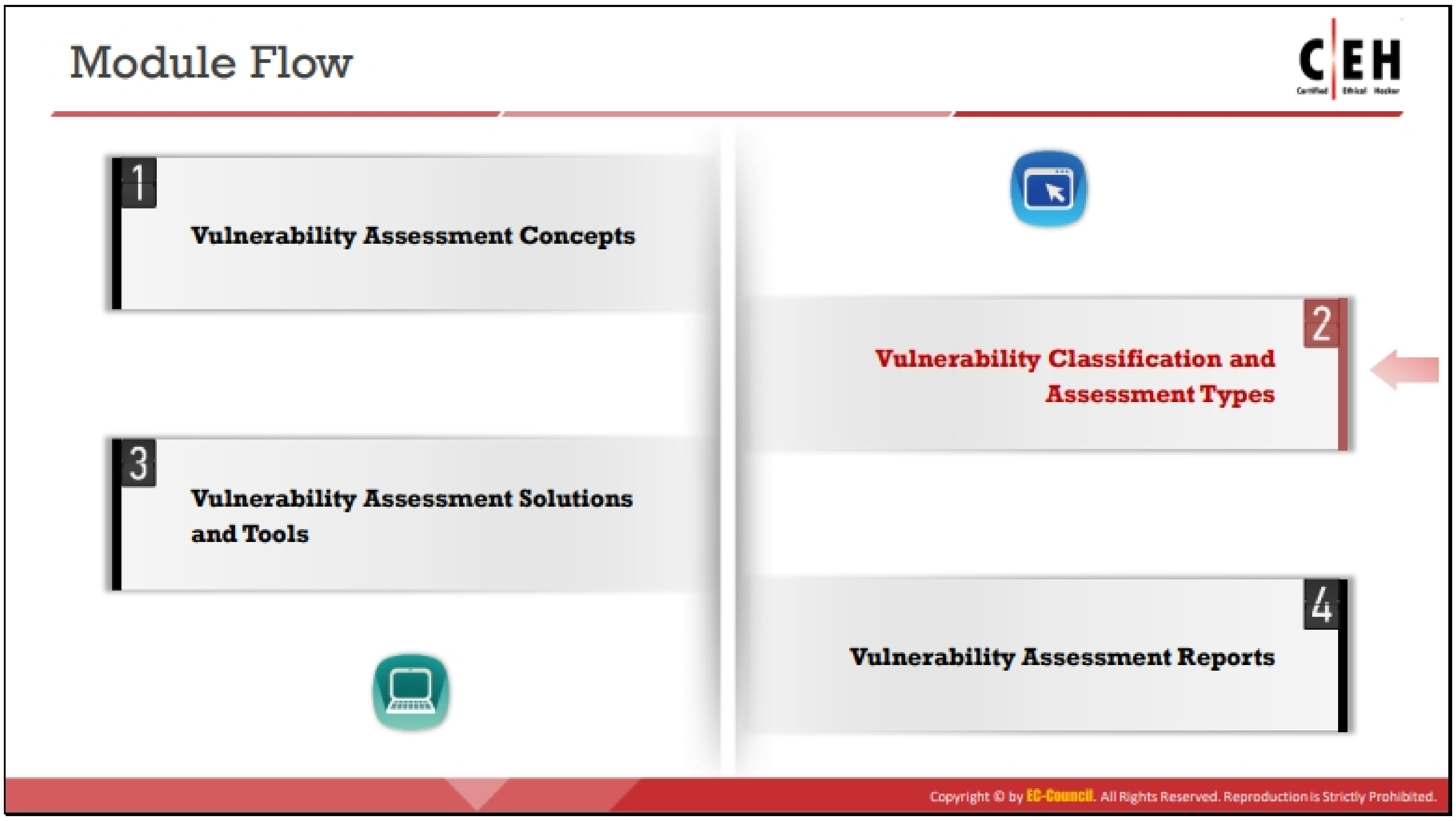
  - Rescanning the systems to identify if an applied fix is effective in remediating the vulnerability
  - Performing dynamic analysis
  - Reviewing the attack surface

- **Monitoring**

  This phase performs incident monitoring using tools such as IDS/IPS, SIEM, and firewalls. It implements continuous security monitoring to thwart ever-evolving threats.

  The tasks performed in the monitoring phase include:

  - Periodic vulnerability scan and assessment
  - Timely remediation of identified vulnerabilities
  - Monitoring intrusion detection and intrusion prevention logs
  - Implementing policies, procedures, and controls



Module Flow

1 **Vulnerability Assessment Concepts**

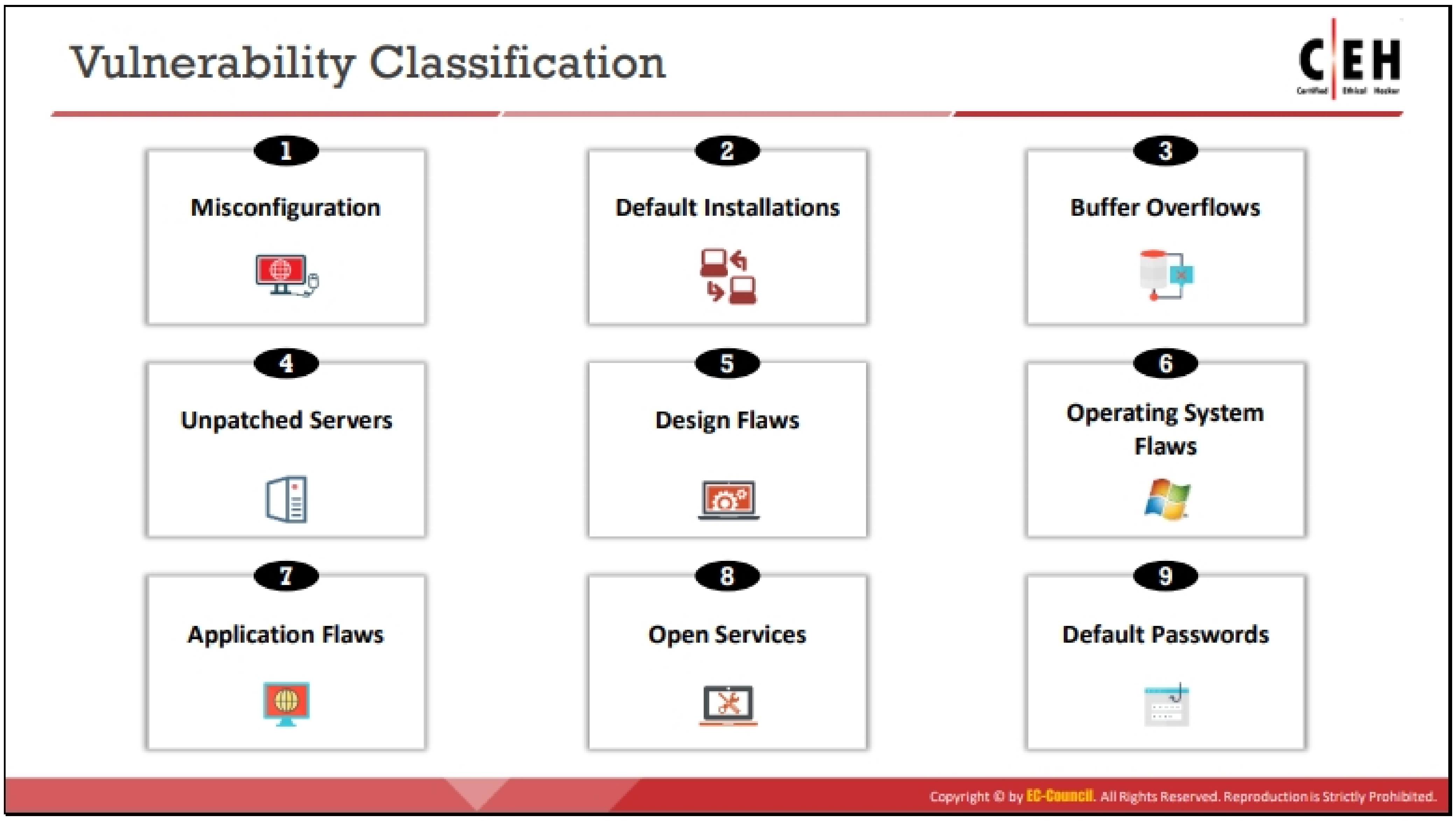
2 **Vulnerability Classification and Assessment Types**

3 **Vulnerability Assessment Solutions and Tools**

4 **Vulnerability Assessment Reports**

Vulnerability Classification and Assessment Types

Any vulnerability that is present in a system can be hazardous and can cause severe damage to the organization. It is important for ethical hackers to have knowledge about various types of vulnerabilities that they can employ, along with various vulnerability assessment techniques. This section in the module discusses the various types of vulnerabilities and vulnerability assessments.



Vulnerability Classification

1 Misconfiguration
2 Default Installations
3 Buffer Overflows
4 Unpatched Servers
5 Design Flaws
6 Operating System Flaws
7 Application Flaws
8 Open Services
9 Default Passwords

Vulnerability Classification

Vulnerabilities present in a system or network are classified into the following categories:

- **Misconfiguration**

  Misconfiguration is the most common vulnerability and is mainly caused by human error, which allows attackers to gain unauthorized access to the system. It may happen intentionally or unintentionally and affects web servers, application platforms, databases, and networks.

  The following are some examples of misconfiguration:

  - An application running with debug enabled
  - Unnecessary administrative ports that are open for an application
  - Running outdated software on the system
  - Running unnecessary services on a machine
  - Outbound connections to various Internet services
  - Using misconfigured SSL certificates or default certificates
  - Improperly authenticated external systems
  - Incorrect folder permissions
  - Default accounts or passwords
  - Set up or configuration pages enabled
  - Disabling security settings and features

Attackers can easily detect these misconfigurations using scanning tools and then exploit the backend systems. Therefore, the administrators must change the default configuration of devices and optimize device security.

- **Default Installations**

  Default installations are usually user-friendly — especially when the device is being used for the first time when the primary concern is the usability of the device rather than the device's security. In some cases, infected devices may not contain any valuable information, but are connected to networks or systems that have confidential information that would result in a data breach. Failing to change the default settings while deploying the software or hardware allows the attacker to guess the settings to break into the system.

- **Buffer Overflows**

  Buffer overflows are common software vulnerabilities that happen due to coding errors that allow attackers to gain access to the target system. In a buffer overflow attack, the attackers undermine the functioning of programs and try to take control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause. The buffer is not able to handle data beyond its limit, causing the flow of data to adjacent memory locations and overwriting their data values. Systems often crash, become unstable, or show erratic program behavior when buffer overflow occurs.

- **Unpatched Servers**

  Servers are an essential component of the infrastructure of any organization. There are several cases where organizations run unpatched and misconfigured servers that compromise the security and integrity of the data in their system. Hackers look out for these vulnerabilities in the servers and exploit them. As these unpatched servers are a hub for the attackers, they serve as an entry point into the network. This can lead to the exposure of private data, financial loss, and discontinuation of operations. Updating software regularly and maintaining systems properly by patching and fixing bugs can help in mitigating the vulnerabilities caused by unpatched servers.

- **Design Flaws**

  Vulnerabilities due to design flaws are universal to all operating devices and systems. Design vulnerabilities such as incorrect encryption or the poor validation of data refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.

- **Operating System Flaws**

  Due to vulnerabilities in the operating systems, applications such as trojans, worms, and viruses pose threats. These attacks use malicious code, script, or unwanted software, which results in the loss of sensitive information and control of computer operations. Timely patching of the OS, installing minimal software applications, and using applications with firewall capabilities are essential steps that an administrator must take to protect the OS from attacks.

- **Application Flaws**

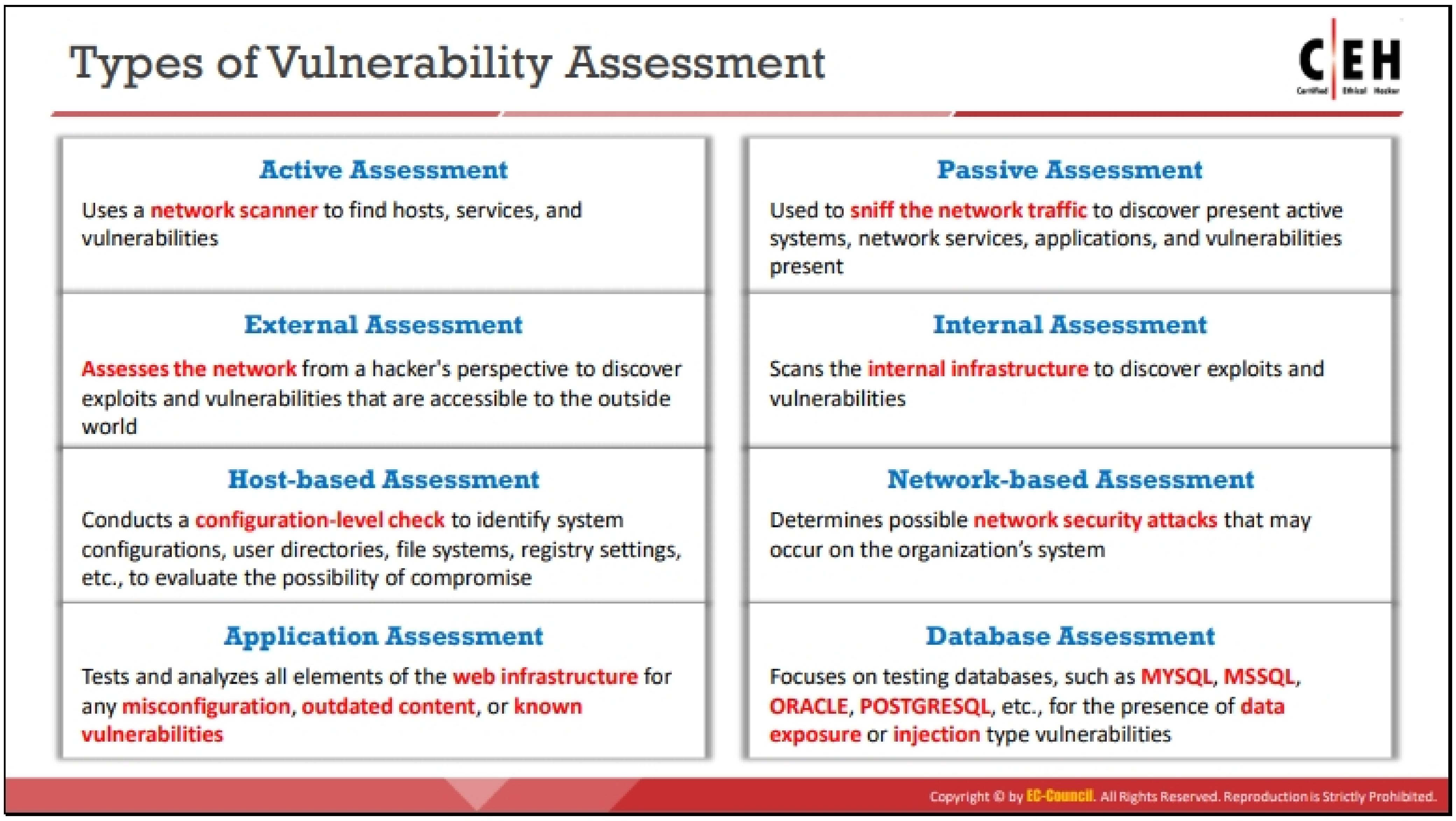
  Application flaws are vulnerabilities in applications that are exploited by the attackers. Applications should be secured using the validation and authorization of the user. Flawed applications pose security threats such as data tampering and unauthorized access to configuration stores. If the applications are not secured, sensitive information may be lost or corrupted. Hence, developers must understand the anatomy of common security vulnerabilities and develop highly secure applications by providing proper user validation and authorization.

- **Open Services**

  Open ports and services may lead to the loss of data or DoS attacks and allow attackers to perform further attacks on other connected devices. Administrators must continuously check for unnecessary or insecure ports and services to reduce the risk to the network.

- **Default Passwords**

  Manufacturers provide users with default passwords to access the device during its initial set-up, which users must change for future use. When users forget to update the passwords and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute force and dictionary attacks. Attackers exploit this vulnerability to obtain access to the system. Passwords should be kept confidential; failing to protect the confidentiality of a password allows the system to be easily compromised.



Types of Vulnerability Assessment

Active Assessment

Uses a network scanner to find hosts, services, and vulnerabilities

Passive Assessment

Used to sniff the network traffic to discover present active systems, network services, applications, and vulnerabilities present

External Assessment

Assesses the network from a hacker's perspective to discover exploits and vulnerabilities that are accessible to the outside world

Internal Assessment

Scans the internal infrastructure to discover exploits and vulnerabilities

Host-based Assessment

Conducts a configuration-level check to identify system configurations, user directories, file systems, registry settings, etc., to evaluate the possibility of compromise

Network-based Assessment

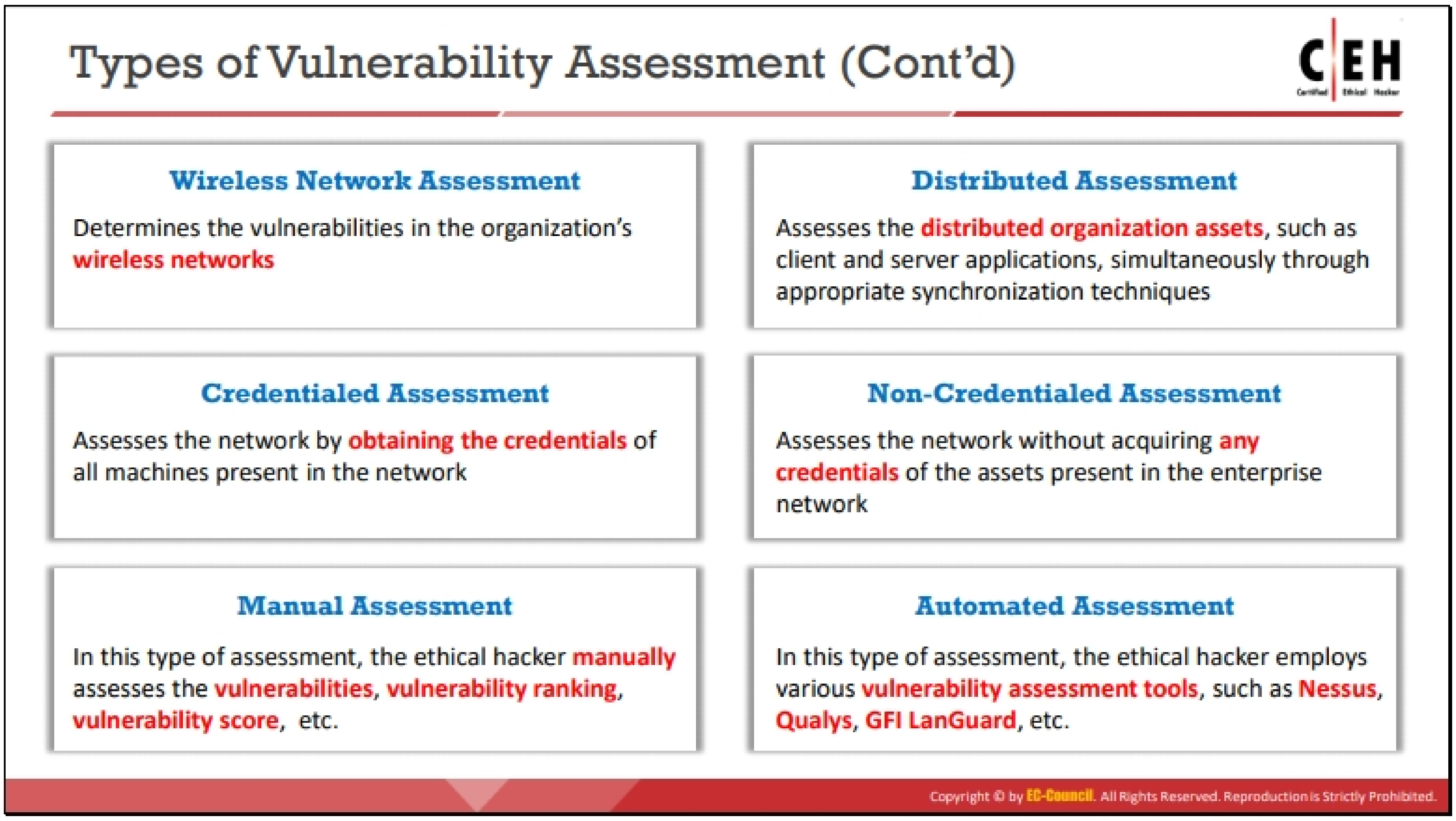
Determines possible network security attacks that may occur on the organization's system

Application Assessment

Tests and analyzes all elements of the web infrastructure for any misconfiguration, outdated content, or known vulnerabilities

Database Assessment

Focuses on testing databases, such as MYSQL, MSSQL, ORACLE, POSTGRESQL, etc., for the presence of data exposure or injection type vulnerabilities



Types of Vulnerability Assessment (Cont'd)

Wireless Network Assessment

Determines the vulnerabilities in the organization's wireless networks

Distributed Assessment

Assesses the distributed organization assets, such as client and server applications, simultaneously through appropriate synchronization techniques

Credentialed Assessment

Assesses the network by obtaining the credentials of all machines present in the network

Non-Credentialed Assessment

Assesses the network without acquiring any credentials of the assets present in the enterprise network

Manual Assessment

In this type of assessment, the ethical hacker manually assesses the vulnerabilities, vulnerability ranking, vulnerability score, etc.

Automated Assessment

In this type of assessment, the ethical hacker employs various vulnerability assessment tools, such as Nessus, Qualys, GFI LanGuard, etc.

Types of Vulnerability Assessment

Given below are the different types of vulnerability assessments:

- **Active Assessment**

  A type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network. Active network scanners can reduce the intrusiveness of the checks they perform.

- **Passive Assessment**

  Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

- **External Assessment**

  External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall.

  The following are some of the possible steps in performing an external assessment:

  - Determine a set of rules for firewall and router configurations for the external network
  - Check whether the external server devices and network devices are mapped
  - Identify open ports and related services on the external network
  - Examine the patch levels on the server and external network devices
  - Review detection systems such as IDS, firewalls, and application-layer protection systems
  - Get information on DNS zones
  - Scan the external network through a variety of proprietary tools available on the Internet
  - Examine Web applications such as e-commerce and shopping cart software for vulnerabilities

- **Internal Assessment**

  An internal assessment involves scrutinizing the internal network to find exploits and vulnerabilities. The following are some of the possible steps in performing an internal assessment:

  - Specify the open ports and related services on network devices, servers, and systems
  - Check the router configurations and firewall rule sets
  - List the internal vulnerabilities of the operating system and server
  - Scan for any trojans that may be present in the internal environment
  - Check the patch levels on the organization's internal network devices, servers, and systems
  - Check for the existence of malware, spyware, and virus activity and document them

  - Evaluate the physical security
  - Identify and review the remote management process and events
  - Assess the file-sharing mechanisms (for example, NFS and SMB/CIFS shares)
  - Examine the antivirus implementation and events

- **Host-based Assessment**

  Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.

- **Network-based Assessment**

  Network assessments determine the possible network security attacks that may occur on an organization's system. These assessments discover network resources and map the ports and services running to various areas on the network. It evaluates the organization's system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewalls and network scanners, such as Nessus. These scanners identify open ports, recognize the services running on those ports, and detect vulnerabilities associated with these services. These assessments help organizations identify points of entry and attack into a network since they follow the path and approach of the hacker. They help organizations determine how systems are vulnerable to Internet and intranet attacks, and how an attacker can gain access to important information. A typical network assessment conducts the following tests on a network:

  - Checks the network topologies for inappropriate firewall configuration
  - Examines the router filtering rules
  - Identifies inappropriately configured database servers
  - Tests individual services and protocols such as HTTP, SNMP, and FTP
  - Reviews HTML source code for unnecessary information
  - Performs bounds checking on variables

- **Application Assessment**

  An application assessment focuses on transactional Web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the webserver infrastructure for any misconfiguration, outdated content, or known vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Database Assessment**

  A database assessment is any assessment focused on testing the databases for the presence of any misconfiguration or known vulnerabilities. These assessments mainly concentrate on testing various database technologies like MYSQL, MSSQL, ORACLE, and POSTGRESQL to identify data exposure or injection type vulnerabilities. Security professionals use both commercial and open-source tools to perform such assessments.

- **Wireless Network Assessment**

  Wireless network assessment determines the vulnerabilities in an organization's wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization's perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

- **Distributed Assessment**

  This type of assessment, employed by organizations that possess assets like servers and clients at different locations, involves simultaneously assessing the distributed organization assets, such as client and server applications, using appropriate synchronization techniques. Synchronization plays a critical role in this type of assessment. By synchronizing the test runs together, all the separate assets situated at multiple locations can be tested at the same time.

- **Credentialed Assessment**

  Credentialed assessment is also called authenticated assessment. In this type of assessment, the ethical hacker possesses the credentials of all machines present in the assessed network. The chances of finding vulnerabilities related to operating systems and applications are higher in credential assessment than in non-credential assessment. This type of assessment is challenging since it is highly unclear who owns particular assets in large enterprises, and even when the ethical hacker identifies the actual owners of the assets, accessing the credentials of these assets is highly tricky since the asset owners generally do not share such confidential information. Also, even if the ethical hacker successfully acquires all required credentials, maintaining the password list is a huge task since there can be issues with things like changed passwords, typing errors, and administrative privileges. Although it is the best way of assessing a target enterprise network for vulnerabilities and is highly reliable, it is a complex assessment that is challenging.

- **Non-Credentialed Assessment**

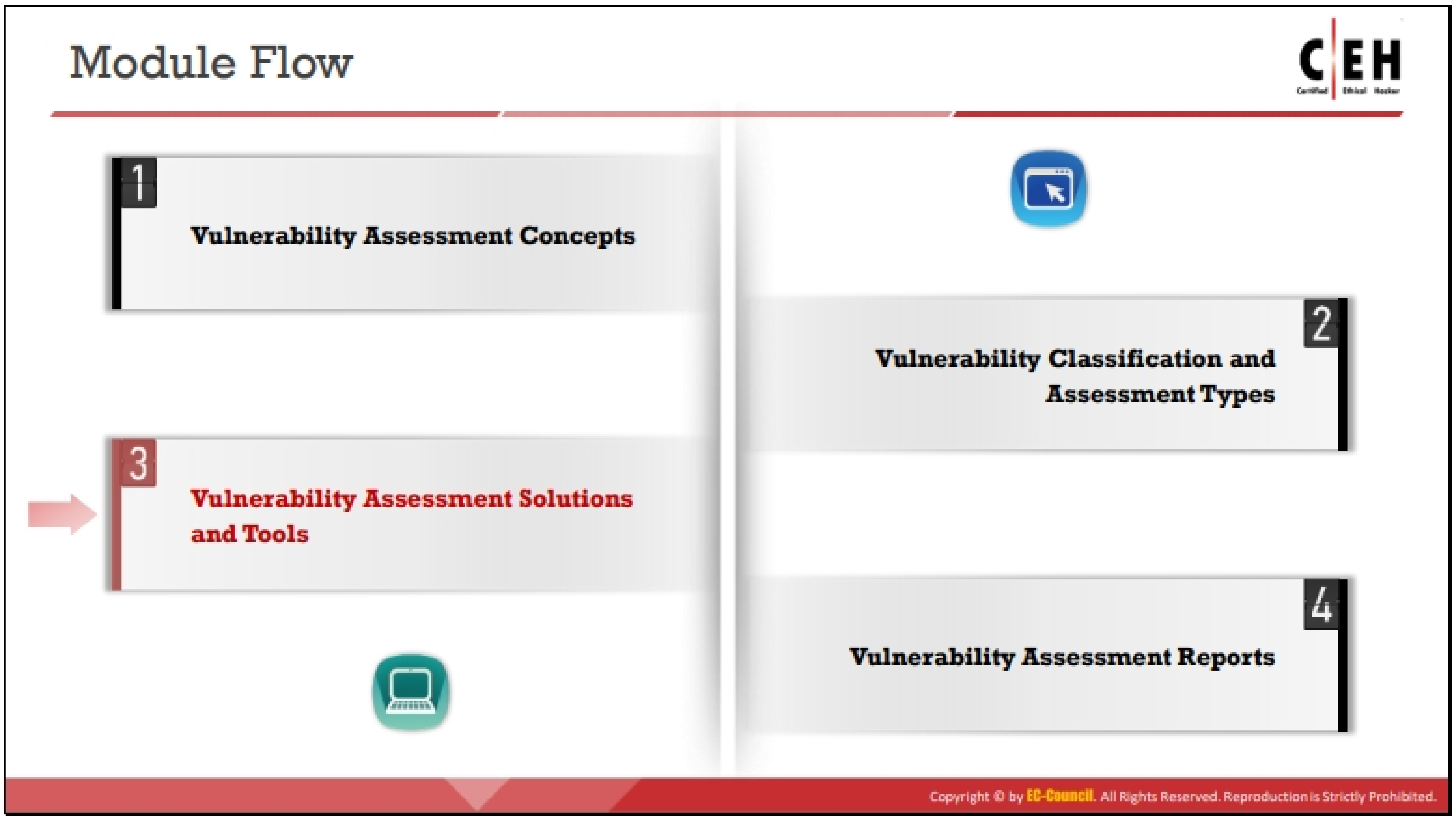
  Non-credentialed assessment, also called unauthenticated assessment, provides a quick overview of weaknesses by analyzing the network services that are exposed by the host. Since it is a non-credential assessment, an ethical hacker does not require any credentials for the assets to perform their assessments. This type of assessment generates a brief report regarding vulnerabilities; however, it is not reliable because it does not provide deeper insight into the OS and application vulnerabilities that are not exposed by the host to the network. This assessment is also incapable of detecting the vulnerabilities that are potentially covered by firewalls. It is prone to false-positive outputs and is not reliably effective as compared to credential-based assessment.

- **Manual Assessment**

  After performing footprinting and network scanning and obtaining crucial information, if the ethical hacker performs manual research for exploring the vulnerabilities or weaknesses, they manually rank the vulnerabilities and score them by referring to vulnerability scoring standards like CVSS and vulnerability databases like CVE and CWE. Such assessment is considered to be manual.

- **Automated Assessment**

  An assessment where an ethical hacker uses vulnerability assessment tools such as Nessus, Qualys, or GFI LanGuard to perform a vulnerability assessment of the target is called an automated assessment. Unlike manual assessments, in this type of assessment, the ethical hacker does not perform footprinting and network scanning. They employ automated tools that can perform all such activities and are also capable of identifying weaknesses and CVSS scores, acquiring critical CVE/CWE information related to the vulnerability, and suggesting remediation strategies.



Module Flow

1 **Vulnerability Assessment Concepts**

2 **Vulnerability Classification and Assessment Types**

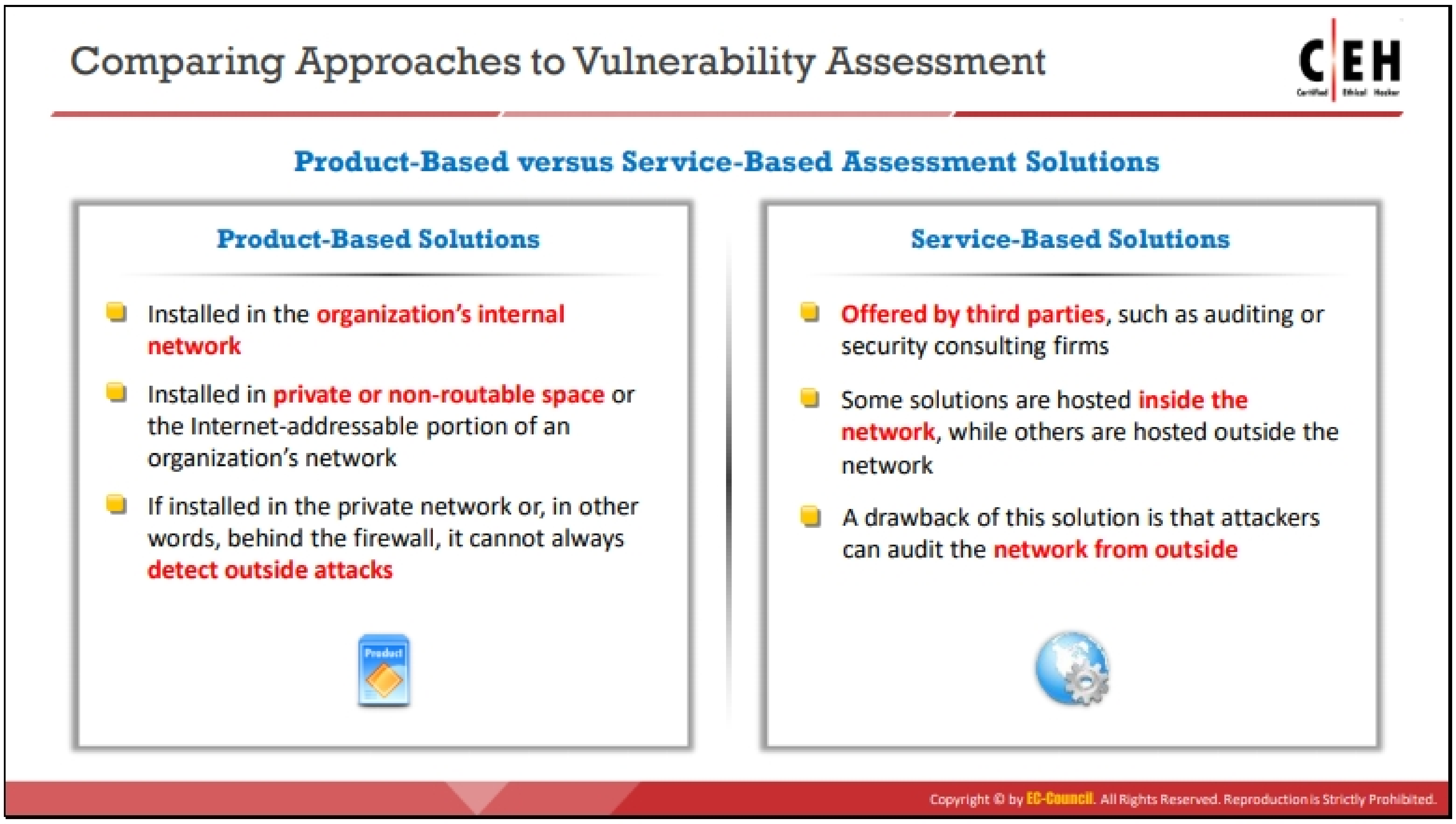
3 **Vulnerability Assessment Solutions and Tools**

4 **Vulnerability Assessment Reports**

Vulnerability Assessment Solutions and Tools

Vulnerability assessment solutions are important tools for information security management as they identify all potential security weaknesses before an attacker can exploit them. There are different approaches and solutions available to perform a vulnerability assessment. Selecting an appropriate assessment approach plays a major role in mitigating the threats that an organization faces.

This section outlines the various approaches, solutions, and tools used to perform a vulnerability assessment.



Comparing Approaches to Vulnerability Assessment

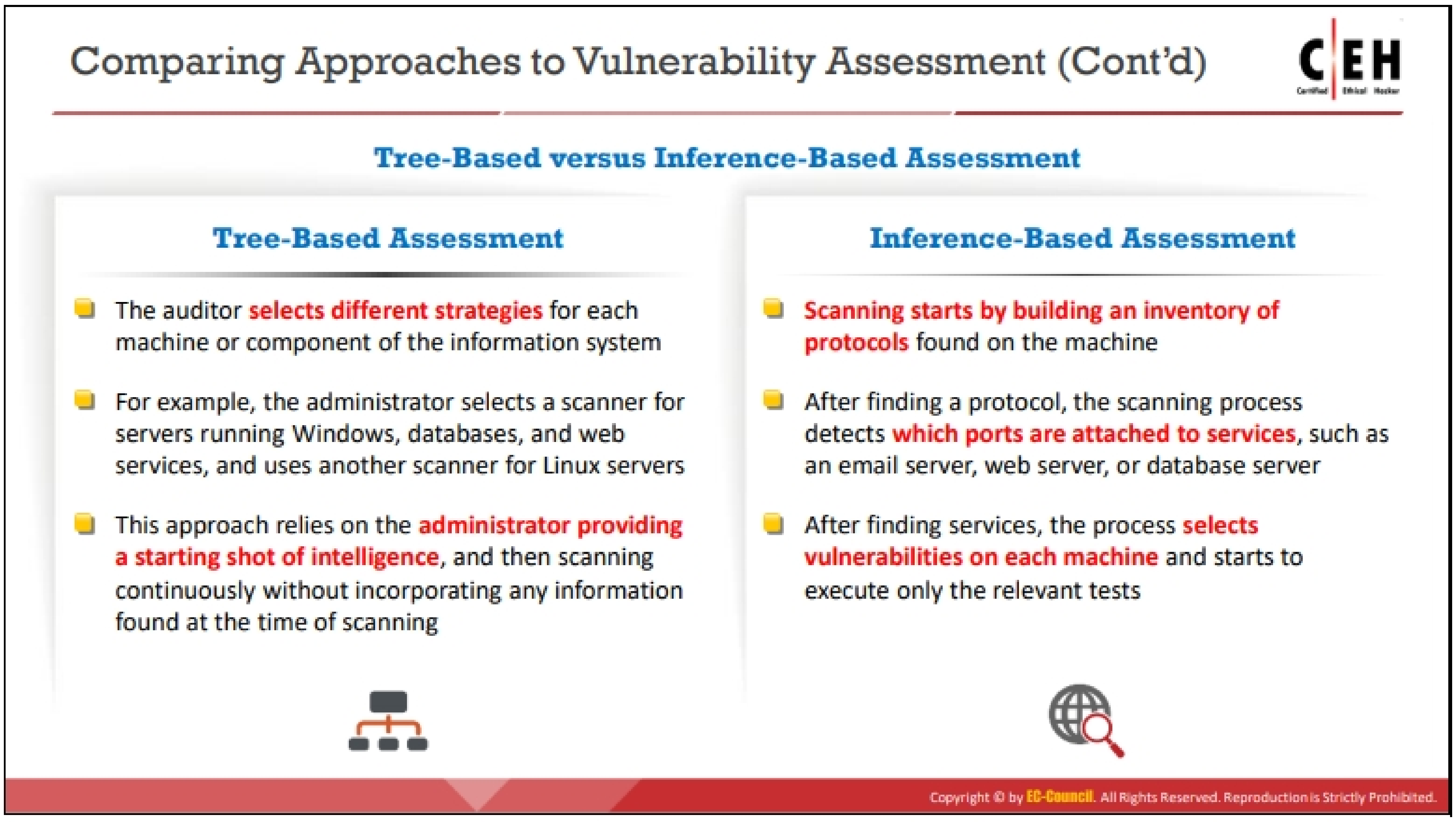
Product-Based versus Service-Based Assessment Solutions

Product-Based Solutions

- Installed in the **organization's internal network**
- Installed in **private or non-routable space** or the Internet-addressable portion of an organization's network
- If installed in the private network or, in other words, behind the firewall, it cannot always **detect outside attacks**

Service-Based Solutions

- **Offered by third parties**, such as auditing or security consulting firms
- Some solutions are hosted **inside the network**, while others are hosted outside the network
- A drawback of this solution is that attackers can audit the **network from outside**



Comparing Approaches to Vulnerability Assessment (Cont'd)

Tree-Based versus Inference-Based Assessment

Tree-Based Assessment

- The auditor **selects different strategies** for each machine or component of the information system
- For example, the administrator selects a scanner for servers running Windows, databases, and web services, and uses another scanner for Linux servers
- This approach relies on the **administrator providing a starting shot of intelligence**, and then scanning continuously without incorporating any information found at the time of scanning

Inference-Based Assessment

- **Scanning starts by building an inventory of protocols** found on the machine
- After finding a protocol, the scanning process detects **which ports are attached to services**, such as an email server, web server, or database server
- After finding services, the process **selects vulnerabilities on each machine** and starts to execute only the relevant tests

Comparing Approaches to Vulnerability Assessment

There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and inference-based assessment.

- **Product-Based Solutions**

  Product-based solutions are installed in the organization's internal network. They are installed either on a private or non-routable space or in the Internet-addressable portion of an organization's network. If they are installed on a private network (behind the firewall), they cannot always detect outside attacks.

- **Service-Based Solutions**

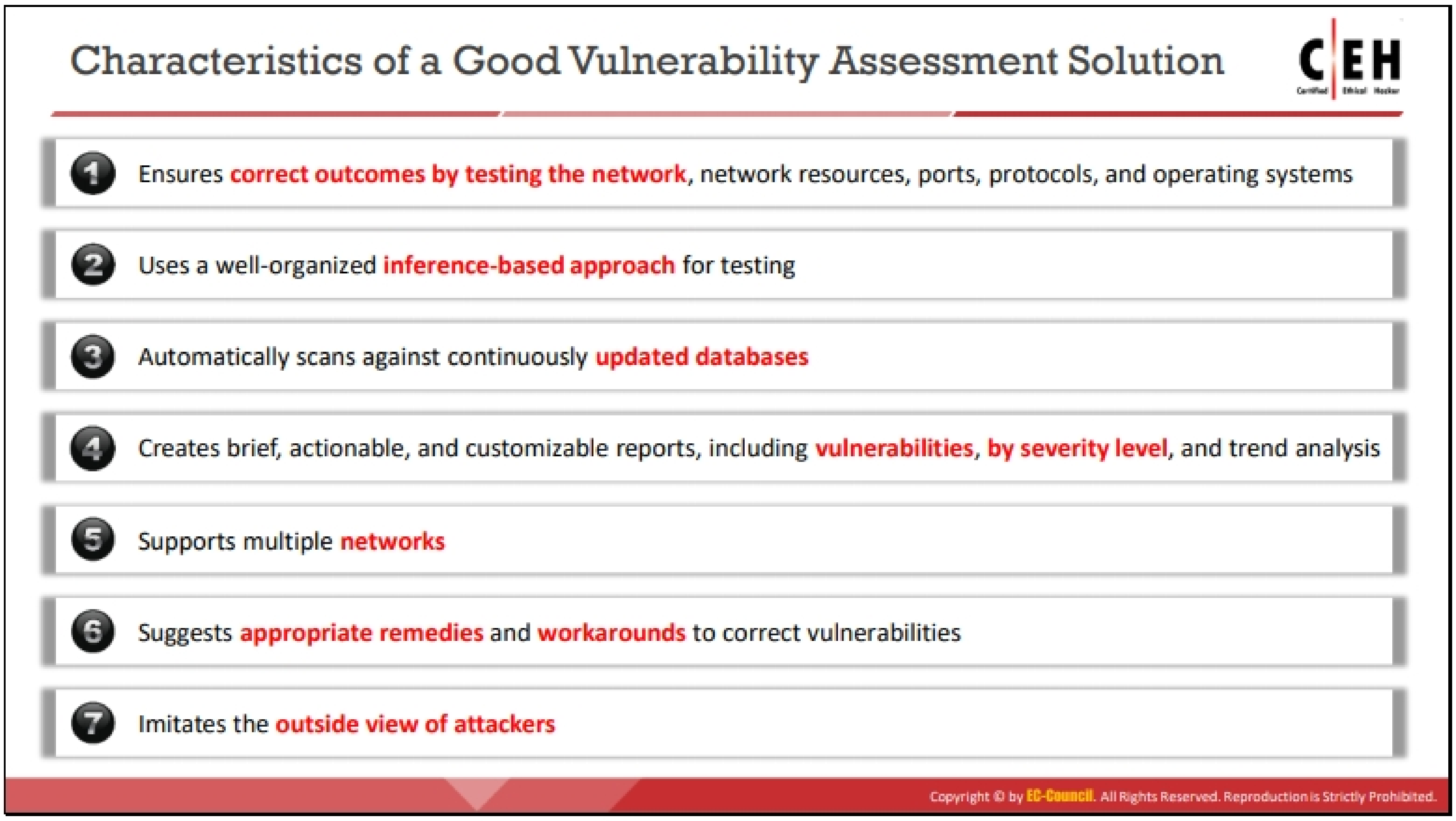
  Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can audit the network from the outside.

- **Tree-Based Assessment**

  In a tree-based assessment, the auditor selects different strategies for each machine or component of the information system. For example, the administrator selects a scanner for servers running Windows, databases, and web services but uses a different scanner for Linux servers. This approach relies on the administrator to provide a starting piece of intelligence, and then to start scanning continuously without incorporating any information found at the time of scanning.

- **Inference-Based Assessment**

  In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.



Characteristics of a Good Vulnerability Assessment Solution

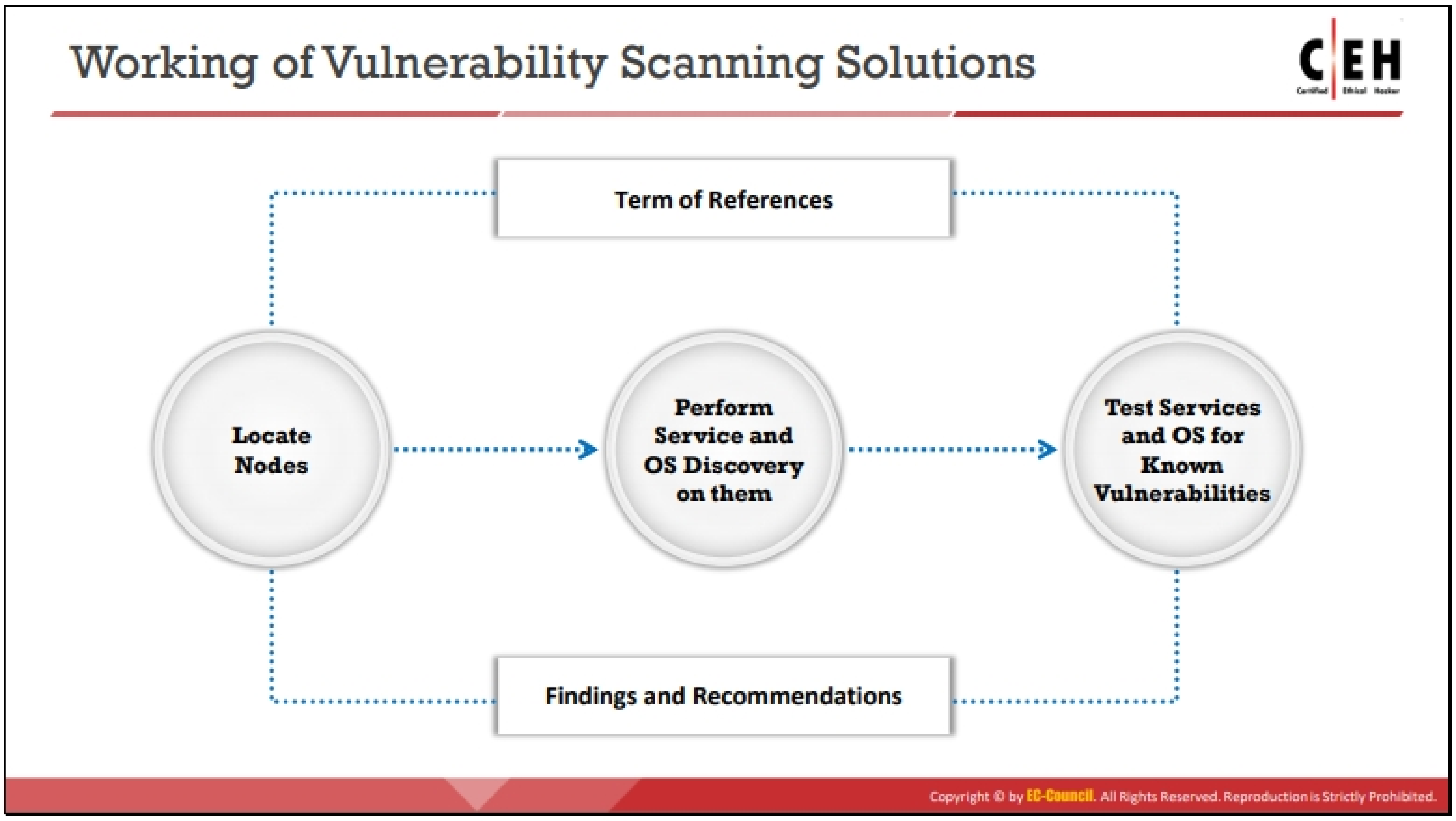
1. Ensures **correct outcomes by testing the network**, network resources, ports, protocols, and operating systems
2. Uses a well-organized **inference-based approach** for testing
3. Automatically scans against continuously **updated databases**
4. Creates brief, actionable, and customizable reports, including **vulnerabilities**, **by severity level**, and trend analysis
5. Supports multiple **networks**
6. Suggests **appropriate remedies** and **workarounds** to correct vulnerabilities
7. Imitates the **outside view of attackers**

Characteristics of a Good Vulnerability Assessment Solution

Organizations need to select a proper and suitable vulnerability assessment solution to detect, assess, and protect their critical IT assets from various internal and external threats.

The characteristics of a good vulnerability assessment solution are as follows:

- Ensures correct outcomes by testing the network, network resources, ports, protocols, and operating systems
- Uses a well-organized inference-based approach for testing
- Automatically scans and checks against continuously updated databases
- Creates brief, actionable, customizable reports, including reports of vulnerabilities by severity level, and trend analysis
- Supports multiple networks
- Suggests appropriate remedies and workarounds to correct vulnerabilities
- Imitates the outside view of attackers to gain its objective



Working of Vulnerability Scanning Solutions

Term of References

Locate Nodes

Perform Service and OS Discovery on them

Test Services and OS for Known Vulnerabilities

Findings and Recommendations

Working of Vulnerability Scanning Solutions

Any organization needs to handle and process large volumes of data to conduct business. These large volumes of data contain privileged information of that particular organization. Attackers try to identify vulnerabilities that they can exploit, and then use these to gain access to critical data for illegal purposes. Vulnerability analysis analyzes and detects risk-prone areas in the organizational network. This analysis uses various tools and reports on the vulnerabilities present in the network.

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

- **Locating nodes**: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
- **Performing service and OS discovery on them**: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services along with the operating system on the target systems.
- **Testing those services and OS for known vulnerabilities**: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

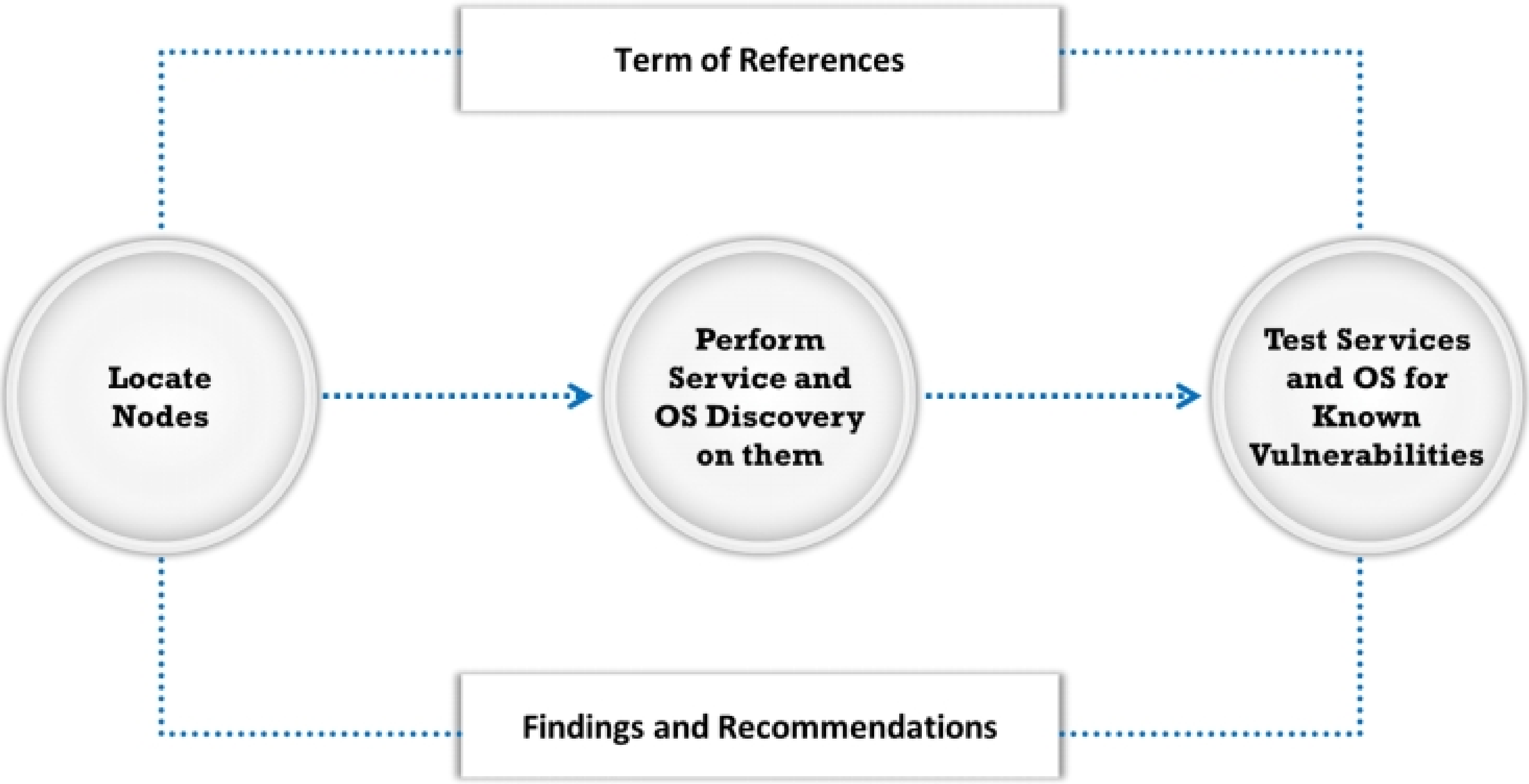
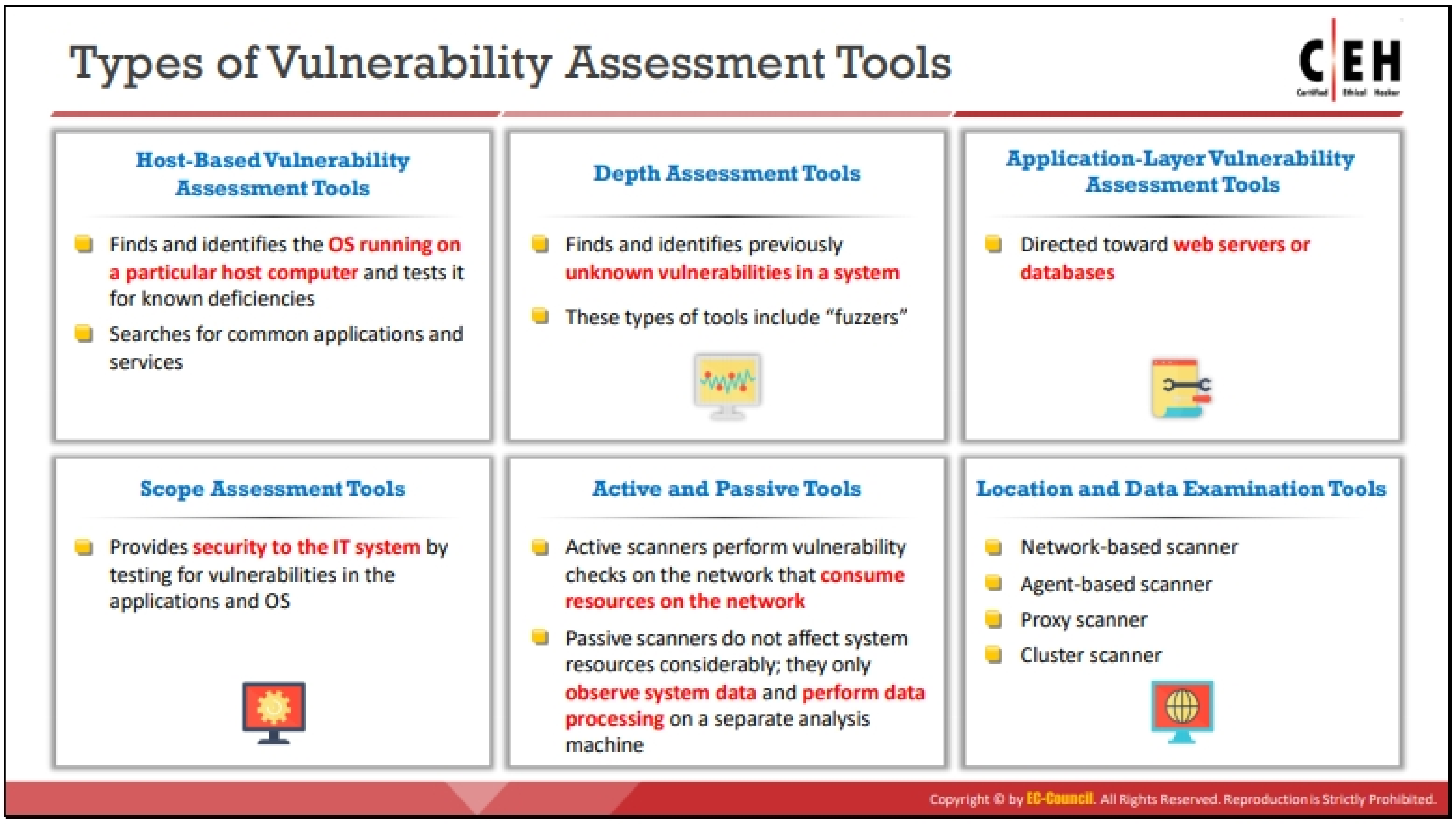

Term of References
Locate Nodes
Perform Service and OS Discovery on them
Test Services and OS for Known Vulnerabilities
Findings and Recommendations

Figure 5.5: The working of vulnerability scanning solutions



Types of Vulnerability Assessment Tools

Host-Based Vulnerability Assessment Tools

- Finds and identifies the **OS running on a particular host computer** and tests it for known deficiencies
- Searches for common applications and services

Depth Assessment Tools

- Finds and identifies previously **unknown vulnerabilities in a system**
- These types of tools include "fuzzers"

Application-Layer Vulnerability Assessment Tools

- Directed toward **web servers or databases**

Scope Assessment Tools

- Provides **security to the IT system** by testing for vulnerabilities in the applications and OS

Active and Passive Tools

- Active scanners perform vulnerability checks on the network that **consume resources on the network**
- Passive scanners do not affect system resources considerably; they only **observe system data** and **perform data processing** on a separate analysis machine

Location and Data Examination Tools

- Network-based scanner
- Agent-based scanner
- Proxy scanner
- Cluster scanner

Types of Vulnerability Assessment Tools

There are six types of vulnerability assessment tools: host-based vulnerability assessment tools, application-layer vulnerability assessment tools, depth assessment tools, scope assessment tools, active and passive tools, and location and data-examination tools.

- **Host-Based Vulnerability Assessment Tools**

  The host-based scanning tools are appropriate for servers that run various applications, such as the Web, critical files, databases, directories, and remote accesses. These host-based scanners can detect high levels of vulnerabilities and provide required information about the fixes (patches). A host-based vulnerability assessment tool identifies the OS running on a particular host computer and tests it for known deficiencies. It also searches for common applications and services.

- **Depth Assessment Tools**

  Depth assessment tools are used to discover and identify previously unknown vulnerabilities in a system. Generally, tools such as fuzzers, which provide arbitrary input to a system's interface, are used to identify vulnerabilities to an unstable depth. Many of these tools use a set of vulnerability signatures to test whether a product is resistant to a known vulnerability or not.

- **Application-Layer Vulnerability Assessment Tools**

  Application-layer vulnerability assessment tools are designed to serve the needs of all kinds of operating system types and applications. Various resources pose a variety of security threats and are identified by the tools designed for that purpose. Observing system vulnerabilities through the Internet using an external router, firewall, or webserver is called an external vulnerability assessment. These vulnerabilities could be external DoS/DDoS threats, network data interception, or other issues. The analyst performs a vulnerability assessment and notes vulnerable resources. The network vulnerability information is updated regularly into the tools. Application-layer vulnerability assessment tools are directed towards web servers or databases.

- **Scope Assessment Tools**

  Scope assessment tools provide an assessment of the security by testing vulnerabilities in the applications and operating system. These tools provide standard controls and a reporting interface that allows the user to select a suitable scan. These tools generate a standard report based on the information found. Some assessment tools are designed to test a specific application or application type for vulnerability.

- **Active and Passive Tools**

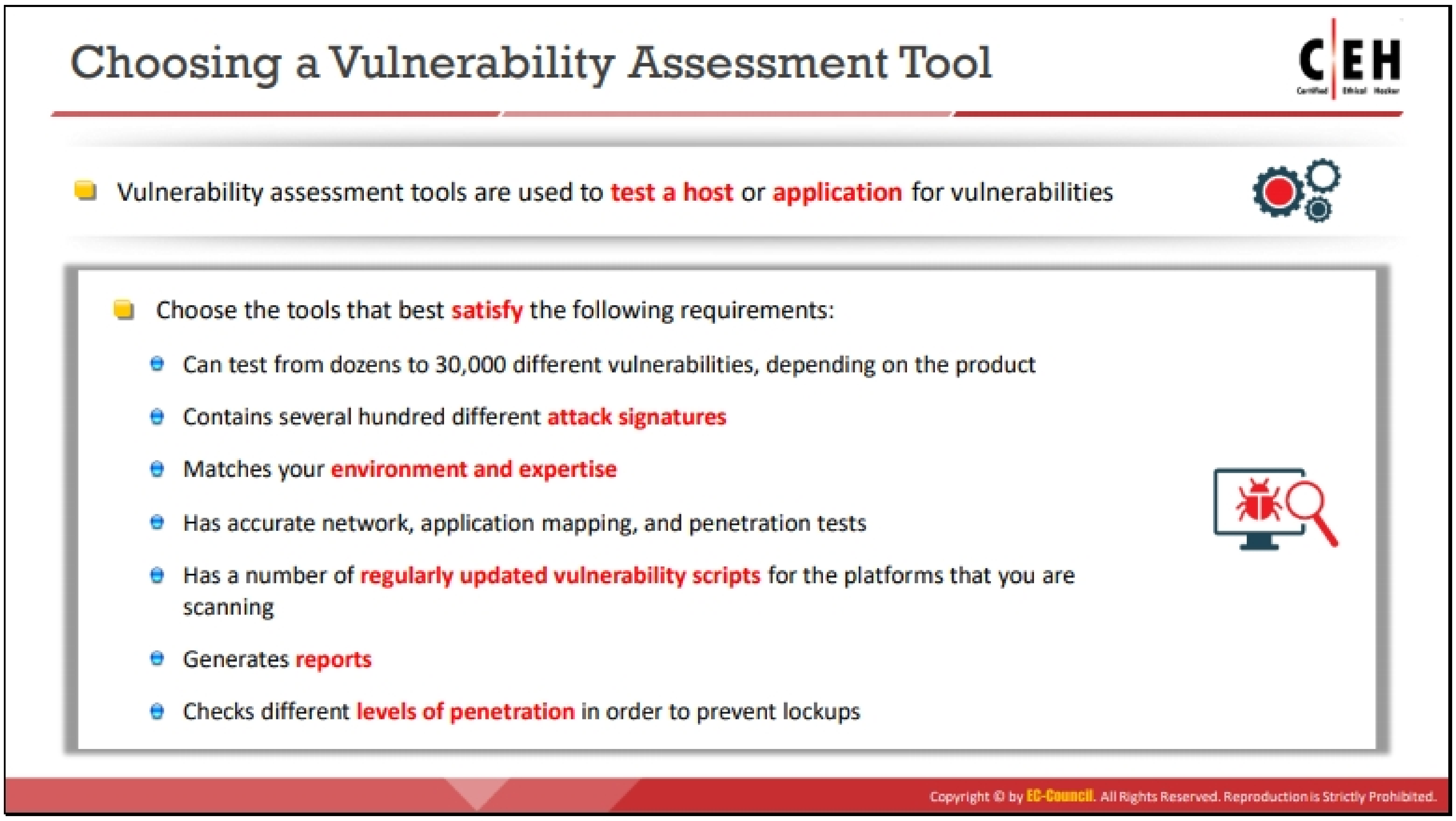
  Active scanners perform vulnerability checks on the network functions that consume resources on the network. The main advantage of the active scanner is that the system administrator or IT manager has good control of the timing and the parameters of vulnerability scans. This scanner cannot be used for critical operating systems because it uses system resources that affect the processing of other tasks.

  Passive scanners are those that do not considerably affect system resources, as they only observe system data and perform data processing on a separate analysis machine. A passive scanner first receives system data that provide complete information on the processes that are running and then assesses that data against a set of rules.

- **Location and Data Examination Tools**

  Listed below are some of the location and data examination tools:

  - **Network-Based Scanner:** Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
  - **Agent-Based Scanner:** Agent-based scanners reside on a single machine but can scan several machines on the same network.
  - **Proxy Scanner:** Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
  - **Cluster scanner:** Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.



Choosing a Vulnerability Assessment Tool

- Vulnerability assessment tools are used to **test a host** or **application** for vulnerabilities

- Choose the tools that best **satisfy** the following requirements:
  - Can test from dozens to 30,000 different vulnerabilities, depending on the product
  - Contains several hundred different **attack signatures**
  - Matches your **environment and expertise**
  - Has accurate network, application mapping, and penetration tests
  - Has a number of **regularly updated vulnerability scripts** for the platforms that you are scanning
  - Generates **reports**
  - Checks different **levels of penetration** in order to prevent lockups

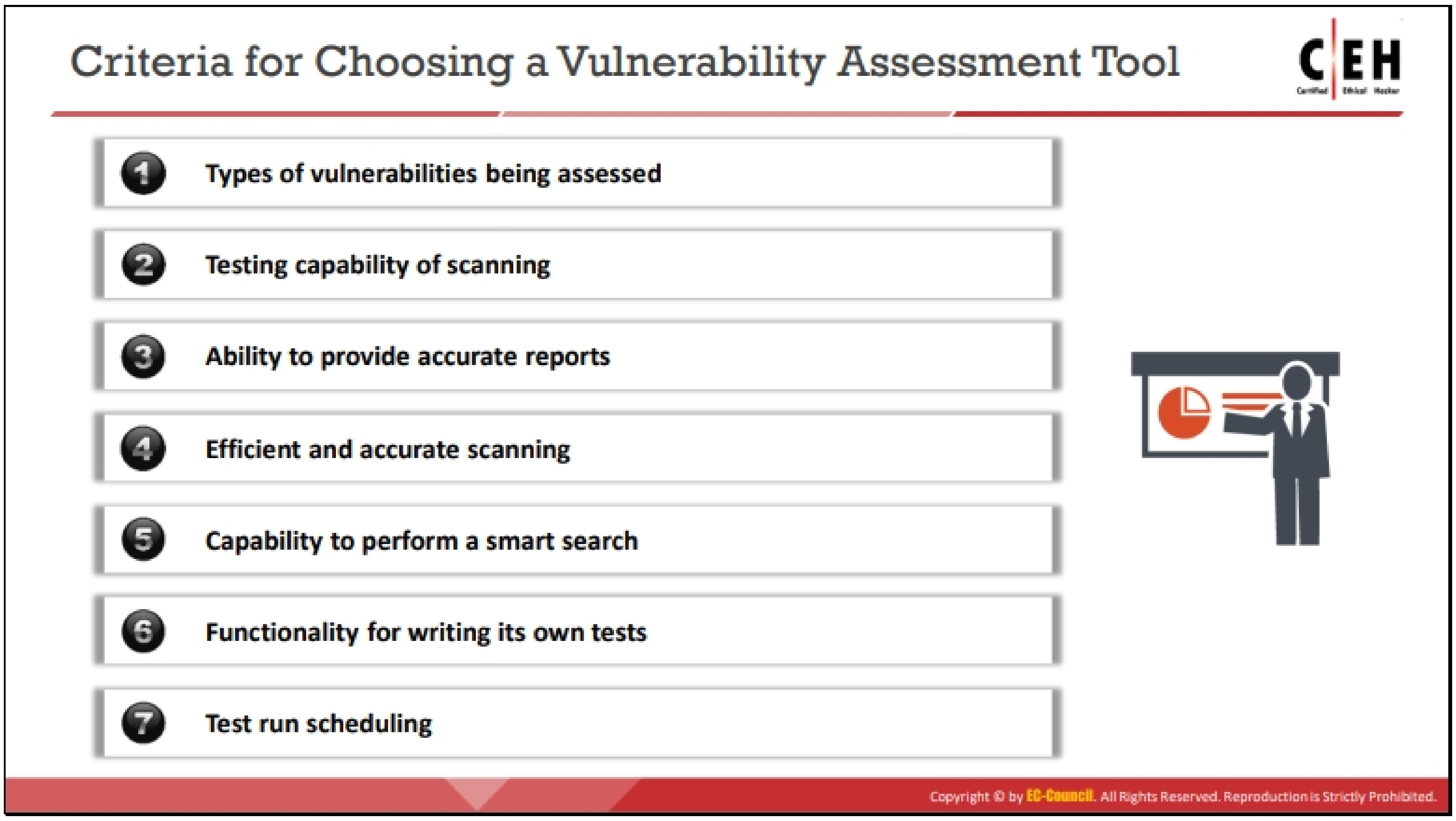
Choosing a Vulnerability Assessment Tool

Vendor-designed vulnerability assessment tools can be used to test a host or application for vulnerabilities. There are several available vulnerability assessment tools that include port scanners, vulnerability scanners, and OS vulnerability assessment scanners. Organizations must choose appropriate tools based on their test requirements.

Choose the tools that best satisfy the following requirements:

- Tools must be capable of testing anywhere from dozens to 30,000 different vulnerabilities, depending on the product
- The selected tool should have a sound database of vulnerabilities and frequently updated attack signatures
- Pick a tool that matches the environment and expertise
- Make sure to regularly update the scan engine to ensure the tool is aware of the latest known vulnerabilities
- Verify that the chosen vulnerability assessment tool has accurate network mapping, application mapping, and penetration tests. Not all tools can find the protocols running and analyze a network's performance.
- Ensure that the tool has several regularly updated vulnerability scripts for the platforms you are scanning
- Make sure that any patches are applied; failing to do so might lead to false positives
- Find out how many reports are returned, what information they contain, and whether they are exportable

- Check whether the tool has different levels of penetration to stop lockups
- The maintenance costs of tools can be offset by effectively using them
- Ensure that the vulnerability assessment tool can run its scans quickly and accurately
- Ensure that the tool can perform scans using multiple protocols
- Verify that the tool can understand and analyze the network topology to perform the assessment
- Bandwidth limitations are a major concern when dealing with large networks. Ensure the vulnerability assessment tool has high bandwidth allocation
- Ensure that the vulnerability assessment tool possess excellent query throttling features
- Ensure that the tool can also assess fragile systems and non-traditional assets



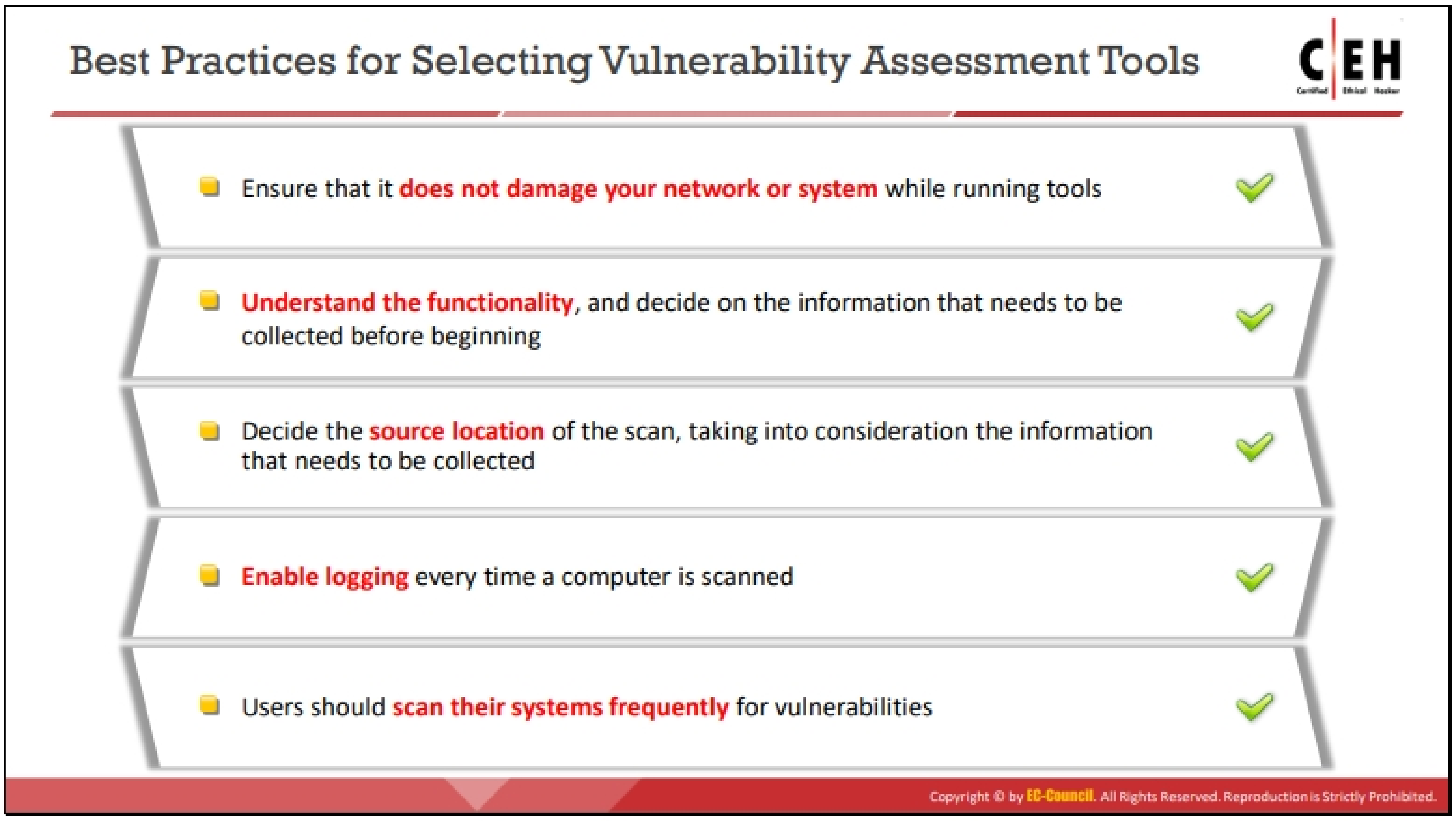
Criteria for Choosing a Vulnerability Assessment Tool

1. Types of vulnerabilities being assessed
2. Testing capability of scanning
3. Ability to provide accurate reports
4. Efficient and accurate scanning
5. Capability to perform a smart search
6. Functionality for writing its own tests
7. Test run scheduling

Criteria for Choosing a Vulnerability Assessment Tool

The criteria to follow when choosing or purchasing any vulnerability assessment tool are as follows:

- **Types of vulnerabilities being assessed**: The most important information at the time of evaluating any tool is to find out how many types of vulnerabilities it will discover.
- **Testing capability of scanning**: The vulnerability assessment tool must have the capacity to execute the entire selected test and must scan all the systems selected for scanning.
- **Ability to provide accurate reports**: The ability to prepare an accurate report is essential. Vulnerability reports should be short, clear, and should provide an easy method to mitigate the discovered vulnerability.
- **Efficient and accurate scanning**: Two essential aspects of scanner performance are how much time it takes for a single host and what resources are required, and the loss of services at the time of scanning. It is important to ensure accuracy and to be aware of the accuracy of the results.
- **Capability to perform a smart search**: How clever they are at the time of scanning is also a key factor in judging any vulnerability assessment tool.
- **Functionality for writing its own tests**: When a signature is not present for a recently found vulnerability, it is helpful if the vulnerability scanning tool allows the use of user-developed tests.
- **Test run scheduling**: It is important to be able to do test-run scheduling as it allows users to perform scanning when traffic on the network is light.



Best Practices for Selecting Vulnerability Assessment Tools

- Ensure that it **does not damage your network or system** while running tools ✓
- **Understand the functionality**, and decide on the information that needs to be collected before beginning ✓
- Decide the **source location** of the scan, taking into consideration the information that needs to be collected ✓
- **Enable logging** every time a computer is scanned ✓
- Users should **scan their systems frequently** for vulnerabilities ✓

Best Practices for Selecting Vulnerability Assessment Tools

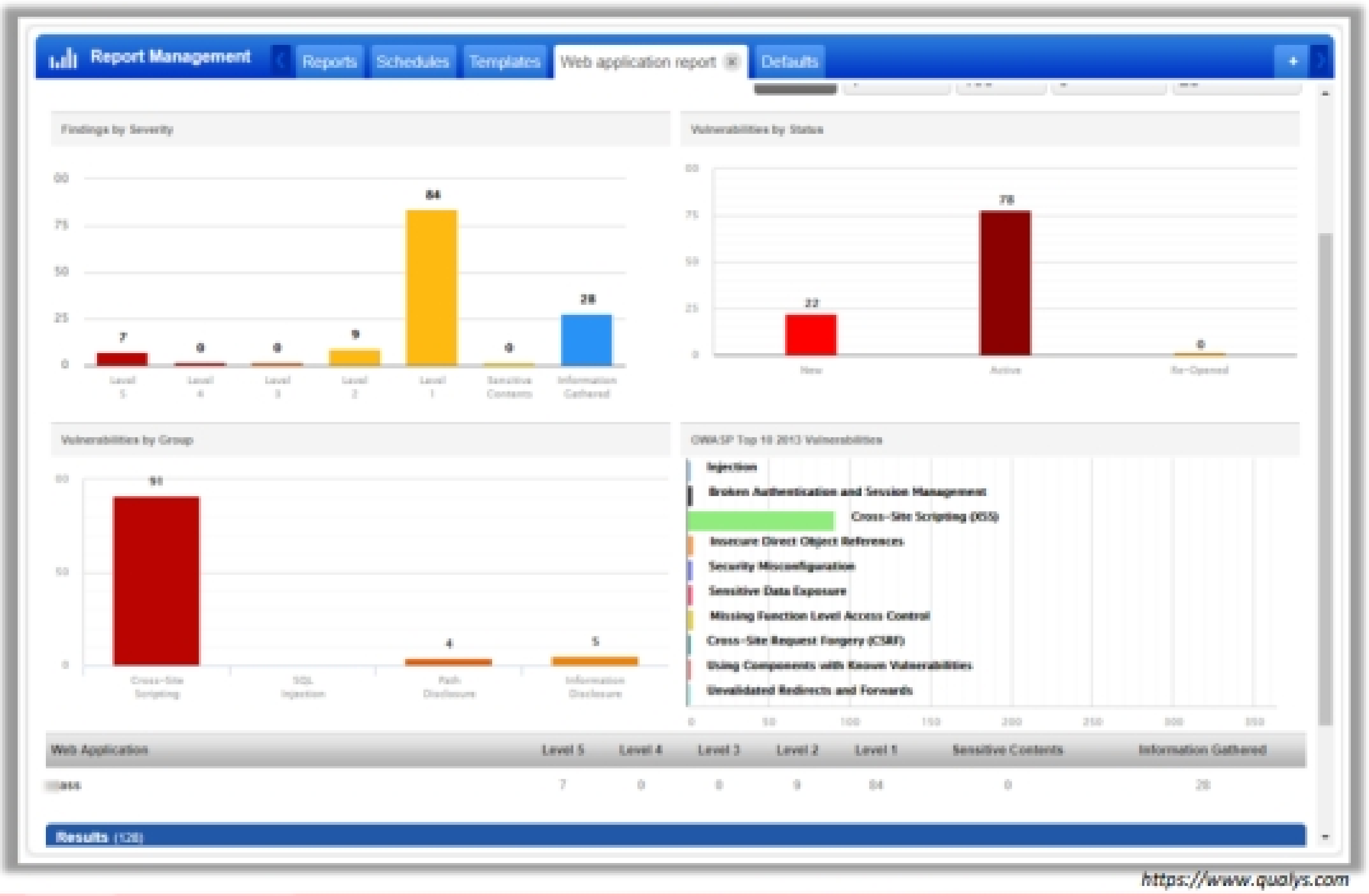
Some of the best practices that can be adopted for selecting vulnerability assessment tools are:

- Vulnerability assessment tools are used to secure and protect the organization's system or network. Ensure that they do not damage the network or system while running.
- Before using any vulnerability assessment tools, it is important to understand their function and to decide what information is needed before starting
- Security mechanisms for accessing from within and from outside the network are somewhat different, so decide the location for the scan based on the desired information
- At the time of scanning, enable logging and ensure that all outcomes and methodologies are annotated every time a scan is performed on any computer
- Users should frequently scan their systems for vulnerabilities and regularly monitor them for vulnerabilities and exploits

Vulnerability Assessment Tools: Qualys Vulnerability Management

- A cloud-based service that offers immediate global visibility into IT system areas that might be **vulnerable to the latest Internet threats** and how to protect them
- Aids in the continuous **identification of threats and monitoring of unexpected changes** in a network before they become breaches

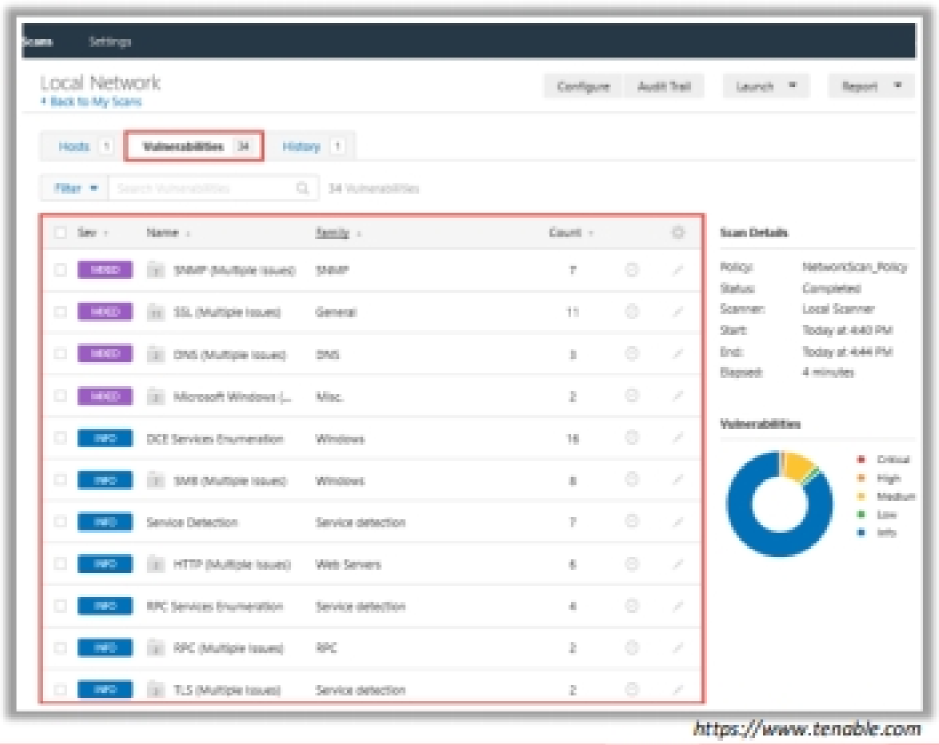
Qualys.


Report Management
Reports
Schedules
Templates
Web application report
Defaults
Findings by Severity
Vulnerabilities by Status
Vulnerabilities by Group
OWASP Top 10 2013 Vulnerabilities
Results (128)

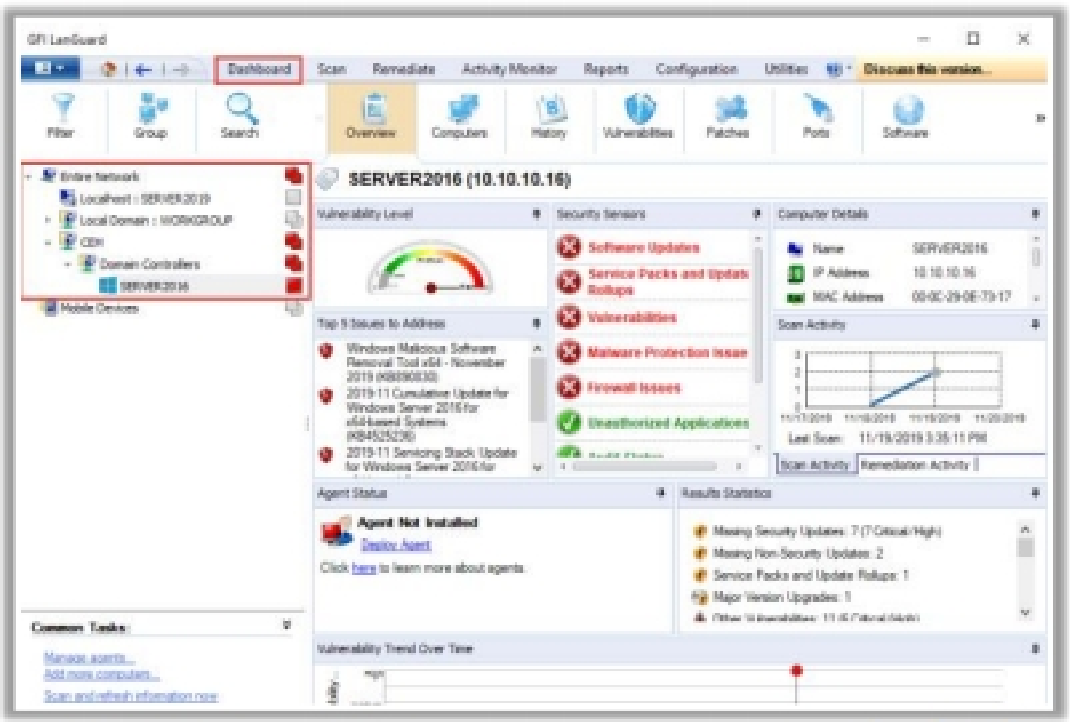
https://www.qualys.com

Vulnerability Assessment Tools: Nessus Professional and GFI LanGuard

Nessus Professional	An assessment solution for **identifying the vulnerabilities, configuration issues,** and **malware**
GFI LanGuard	Scans, detects, assesses, and rectifies **security vulnerabilities** in a network and connected devices


Scans
Settings
Local Network
Hosts
Vulnerabilities
History
Scan Details
Vulnerabilities

https://www.tenable.com

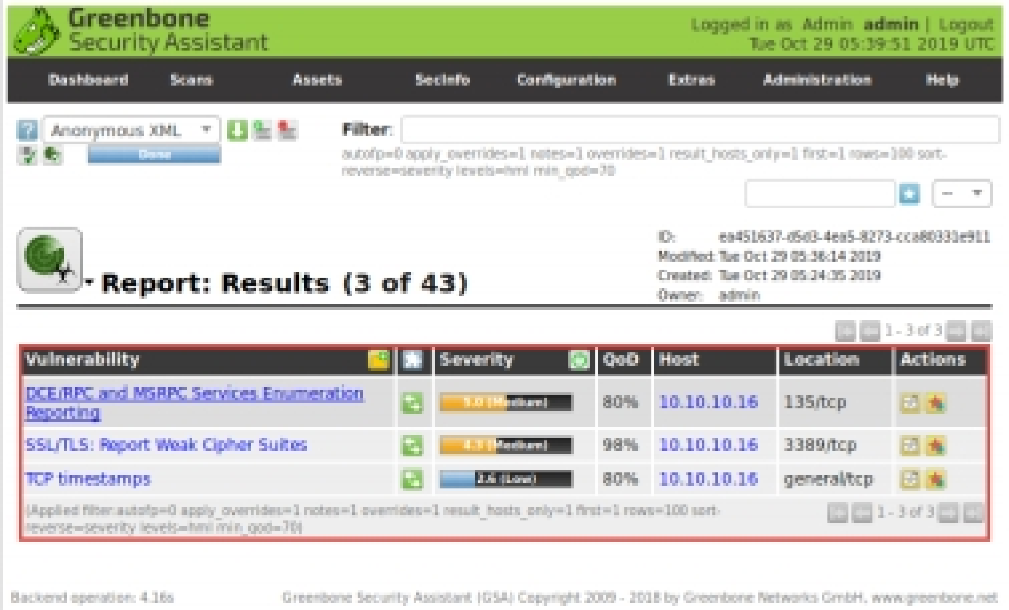

GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
SERVER2016 (10.10.10.16)
Vulnerability Level
Security Sensors
Computer Details
Software Updates
Vulnerabilities
Malware Protection Issue
Firewall Issues
Agent Status
Results Statistics

https://www.gfi.com

Vulnerability Assessment Tools: OpenVAS and Nikto

OpenVAS | A framework of several services and tools offering a comprehensive and powerful **vulnerability scanning** and **vulnerability management solution**

Nikto | A **web server assessment tool** that examines a web server to discover potential problems and security vulnerabilities



autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (3 of 43)

ID: ea451637-d5d3-4ea5-8273-cca80331e911
Modified: Tue Oct 29 05:36:14 2019
Created: Tue Oct 29 05:24:35 2019
Owner: admin

1 - 3 of 3

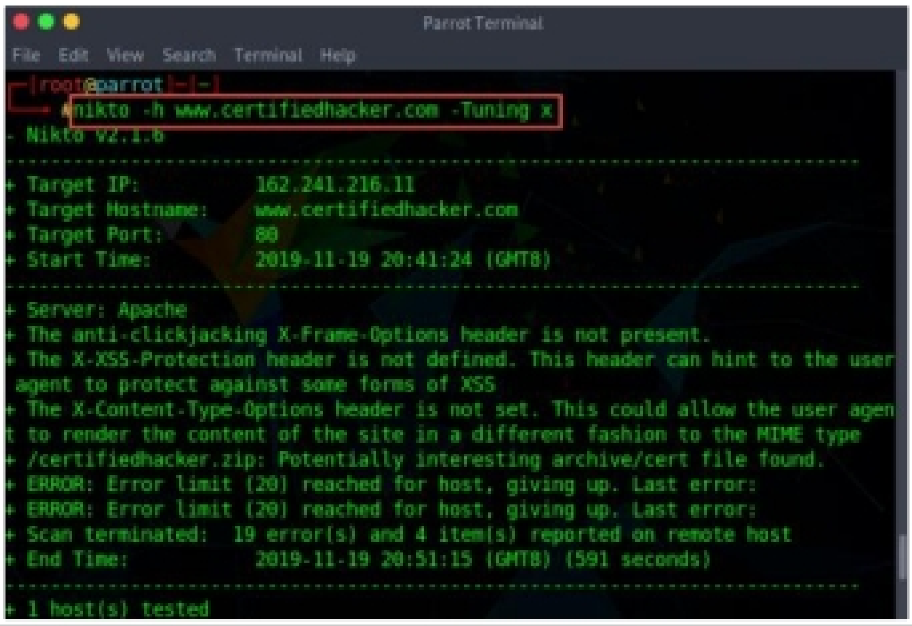
Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.10.10.16	135/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.10.10.16	3389/tcp	
TCP timestamps		2.6 (Low)	80%	10.10.10.16	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

Backend operation: 4.16s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

http://www.openvas.org



```
┌─[root@parrot]─[~]
└──╼ #nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-11-19 20:41:24 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
 agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  19 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-11-19 20:51:15 (GMT8) (591 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

https://cirt.net

Other Vulnerability Assessment Tools

- **Qualys FreeScan**
  https://freescan.qualys.com
- **Acunetix Web Vulnerability Scanner**
  https://www.acunetix.com
- **Nexpose**
  https://www.rapid7.com
- **Network Security Scanner**
  https://www.beyondtrust.com
- **SAINT**
  https://www.saintcorporation.com
- **Microsoft Baseline Security Analyzer (MBSA)**
  https://www.microsoft.com
- **beSECURE (AVDS)**
  https://www.beyondsecurity.com
- **Core Impact Pro**
  https://www.coresecurity.com
- **N-Stalker Web Application Security Scanner**
  https://www.nstalker.com
- **ManageEngine Vulnerability Manager Plus**
  https://www.manageengine.com

Vulnerability Assessment Tools

An attacker performs vulnerability scanning to identify security loopholes in the target network that they can exploit to launch attacks. Security analysts can use vulnerability assessment tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them.

Network vulnerability scanners help to analyze and identify vulnerabilities in the target network or network resources by using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

The following are some of the most effective vulnerability assessment tools:

- **Qualys Vulnerability Management**

  Source: *https://www.qualys.com*

  Qualys VM is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.

  Features:

  - **Agent-based detection**

    Also works with the Qualys Cloud Agents, extending its network coverage to unscannable assets.

  - **Constant monitoring and alerts**

    When VM is paired with Continuous Monitoring (CM), InfoSec teams are proactively alerted about potential threats, so problems can be tackled before they turn into breaches.

  - **Comprehensive coverage and visibility**

    Continuously scans and identifies vulnerabilities for protecting IT assets on-premises, in the cloud, and at mobile endpoints. Its executive dashboard displays an overview of the security posture and gives access to remediation details. VM generates custom, role-based reports for multiple stakeholders, including automatic security documentation for compliance auditors.

  - **VM for the perimeter-less world**

    As enterprises adopt cloud computing, mobility, and other disruptive technologies for digital transformation, Qualys VM offers next-generation vulnerability management for these hybrid IT environments whose traditional boundaries have been blurred.

  - **Discover forgotten devices and organize the host assets**

    Qualys can help quickly determine what is running in different parts of the network—from the perimeter and corporate network to virtualized machines and cloud services. It can also identify unexpected access points, web servers, and other devices that can expose the network to attack.

  - **Scan for vulnerabilities everywhere, accurately and efficiently**

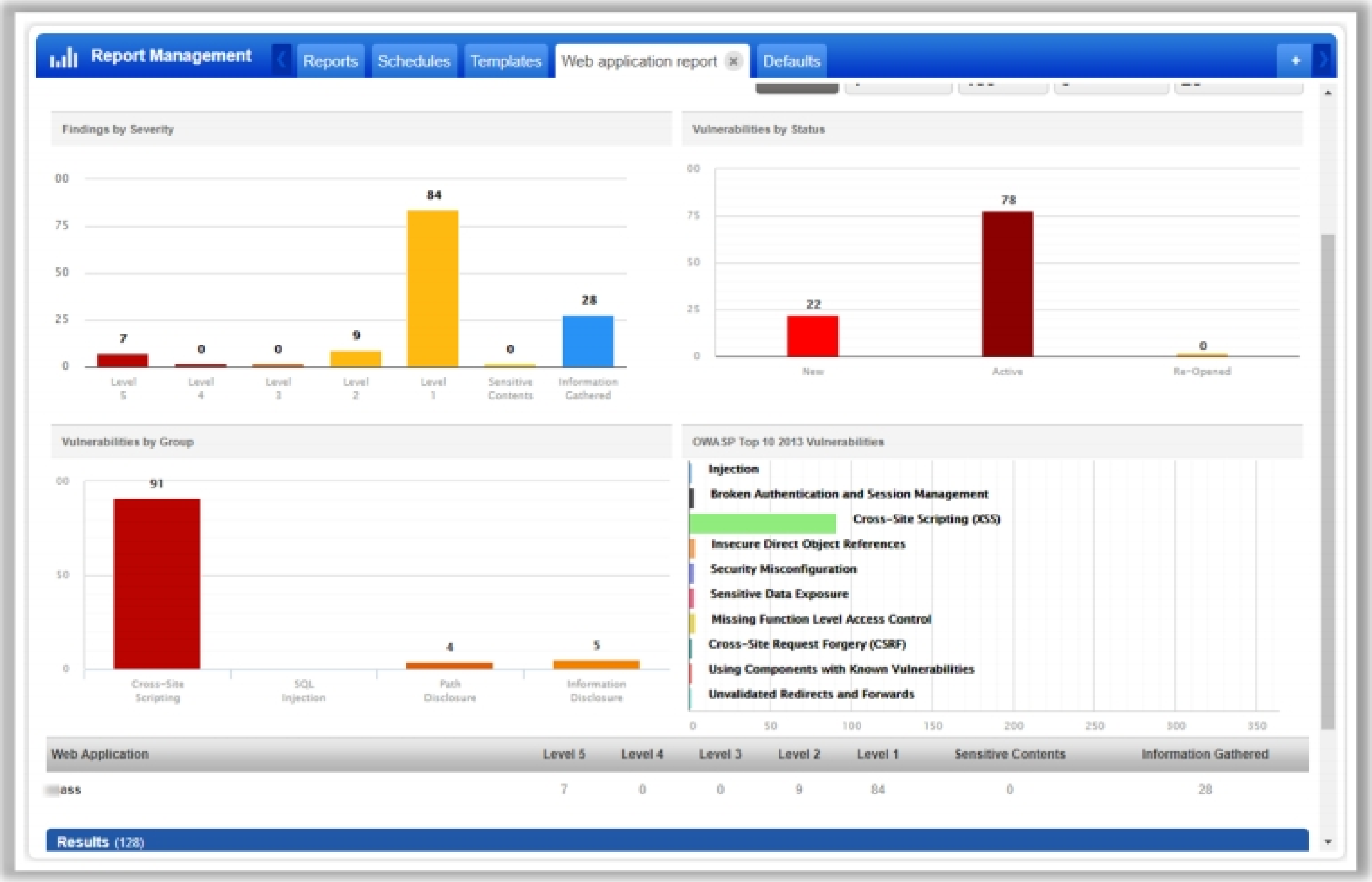
    Scan systems anywhere from the same console, including the perimeter, the internal network, and cloud environments.

- **Identify and prioritize risks**

  Qualys, using trend analysis, Zero-Day, and Patch impact predictions, can identify the highest business risks.

- **Remediate vulnerabilities**

  Qualys's ability to track vulnerability data across hosts and time produces interactive reports that provide a better understanding of the security of the network.


Report Management
Reports
Schedules
Templates
Web application report
Defaults
Findings by Severity
00
75
50
25
0
7
0
0
9
84
0
28
Level 5
Level 4
Level 3
Level 2
Level 1
Sensitive Contents
Information Gathered
Vulnerabilities by Status
00
75
50
25
0
22
78
0
New
Active
Re-Opened
Vulnerabilities by Group
00
50
0
91
4
5
Cross-Site Scripting
SQL Injection
Path Disclosure
Information Disclosure
OWASP Top 10 2013 Vulnerabilities
Injection
Broken Authentication and Session Management
Cross-Site Scripting (XSS)
Insecure Direct Object References
Security Misconfiguration
Sensitive Data Exposure
Missing Function Level Access Control
Cross-Site Request Forgery (CSRF)
Using Components with Known Vulnerabilities
Unvalidated Redirects and Forwards
0
50
100
150
200
250
300
350
Results (128)

Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
[redacted]ass	7	0	0	9	84	0	28

Figure 5.6: Vulnerability scanning using Qualys Vulnerability Management

- **Nessus Professional**

  Source: *https://www.tenable.com*

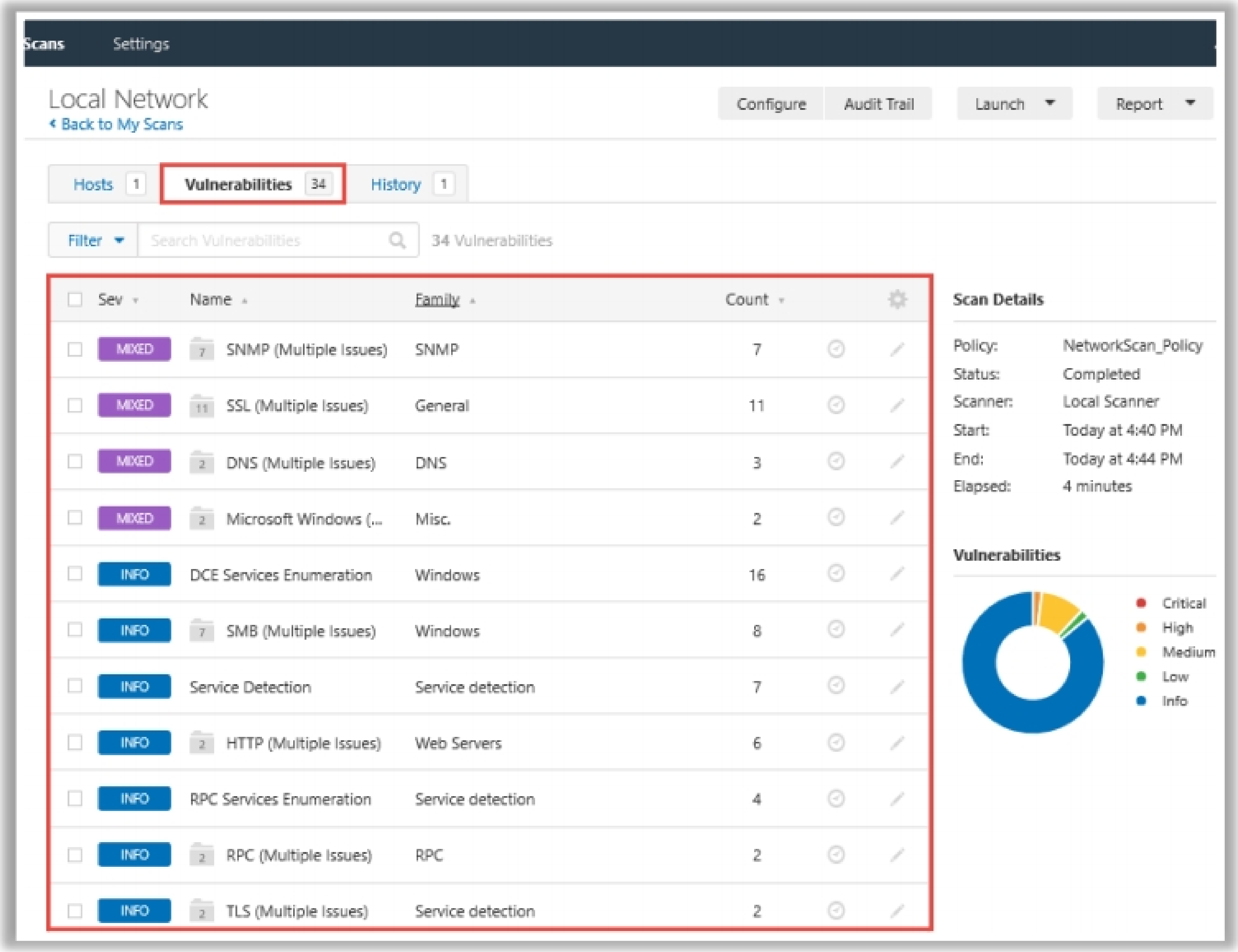
  Nessus Professional is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as operating systems, network devices, hypervisors, databases, tablets and phones, web servers, and critical infrastructure.

  Nessus is the vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, and use wizards to easily and quickly create policies, schedule scans, and send results via email.

  Features:

  - High-speed asset discovery

- Vulnerability assessment
- Malware and Botnet detection
- Configuration and compliance auditing
- Scanning and auditing virtualized and cloud platforms


Scans
Settings
Local Network
‹ Back to My Scans
Configure
Audit Trail
Launch
Report
Hosts 1
Vulnerabilities 34
History 1
Filter
Search Vulnerabilities
34 Vulnerabilities
Critical
High
Medium
Low
Info

☐	Sev	Name	Family	Count
☐	MIXED	SNMP (Multiple Issues)	SNMP	7
☐	MIXED	SSL (Multiple Issues)	General	11
☐	MIXED	DNS (Multiple Issues)	DNS	3
☐	MIXED	Microsoft Windows (...	Misc.	2
☐	INFO	DCE Services Enumeration	Windows	16
☐	INFO	SMB (Multiple Issues)	Windows	8
☐	INFO	Service Detection	Service detection	7
☐	INFO	HTTP (Multiple Issues)	Web Servers	6
☐	INFO	RPC Services Enumeration	Service detection	4
☐	INFO	RPC (Multiple Issues)	RPC	2
☐	INFO	TLS (Multiple Issues)	Service detection	2

Scan Details

Policy: NetworkScan_Policy
Status: Completed
Scanner: Local Scanner
Start: Today at 4:40 PM
End: Today at 4:44 PM
Elapsed: 4 minutes

Vulnerabilities

Figure 5.7: Vulnerability scanning using Nessus

- **GFI LanGuard**

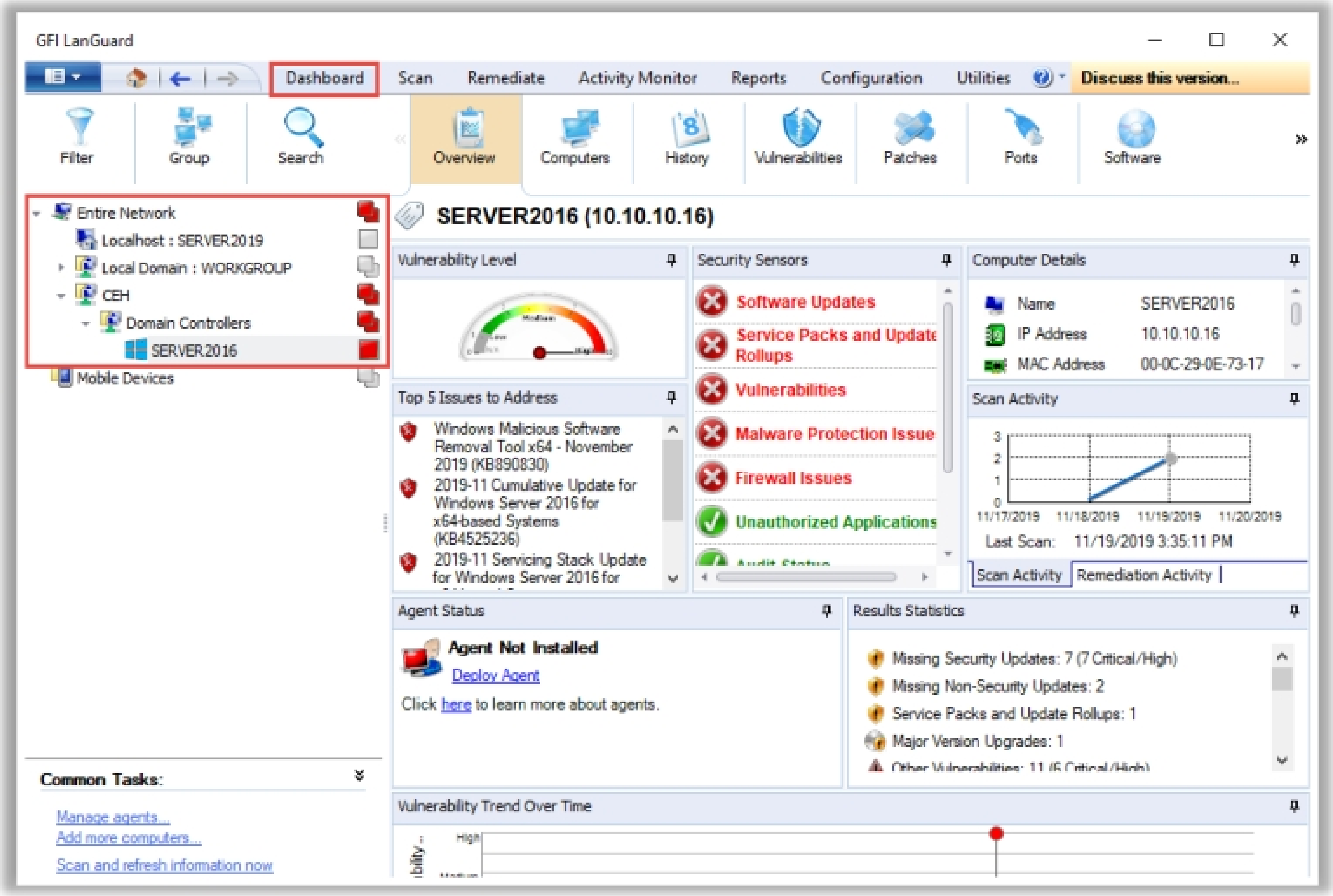
  Source: *https://www.gfi.com*

  GFI LanGuard scans for, detects, assesses, and rectifies security vulnerabilities in a network and its connected devices. This is done with minimal administrative effort. It scans the operating systems, virtual environments, and installed applications through vulnerability check databases. It enables analysis of the state of network security, identifies risks, and offers solutions before the system can be compromised.

  Features:

  - Patch management for operating systems and third-party applications
  - Vulnerability assessment

- A Web reporting console
- Track latest vulnerabilities and missing updates
- Integration with security applications
- Network device vulnerability checks
- Network and software auditing
- Support for virtual environments


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Entire Network
Localhost : SERVER2019
Local Domain : WORKGROUP
CEH
Domain Controllers
SERVER2016
Mobile Devices
SERVER2016 (10.10.10.16)
Vulnerability Level
Security Sensors
Computer Details
Software Updates
Service Packs and Update Rollups
Vulnerabilities
Malware Protection Issue
Firewall Issues
Unauthorized Applications
Top 5 Issues to Address
Scan Activity
Remediation Activity
Agent Status
Results Statistics
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Vulnerability Trend Over Time
High
Medium

Name SERVER2016
IP Address 10.10.10.16
MAC Address 00-0C-29-0E-73-17

Windows Malicious Software Removal Tool x64 - November 2019 (KB890830)
2019-11 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4525236)
2019-11 Servicing Stack Update for Windows Server 2016 for

11/17/2019 11/18/2019 11/19/2019 11/20/2019
Last Scan: 11/19/2019 3:35:11 PM

Agent Not Installed
Deploy Agent
Click here to learn more about agents.

Missing Security Updates: 7 (7 Critical/High)
Missing Non-Security Updates: 2
Service Packs and Update Rollups: 1
Major Version Upgrades: 1
Other Vulnerabilities: 11 (6 Critical/High)

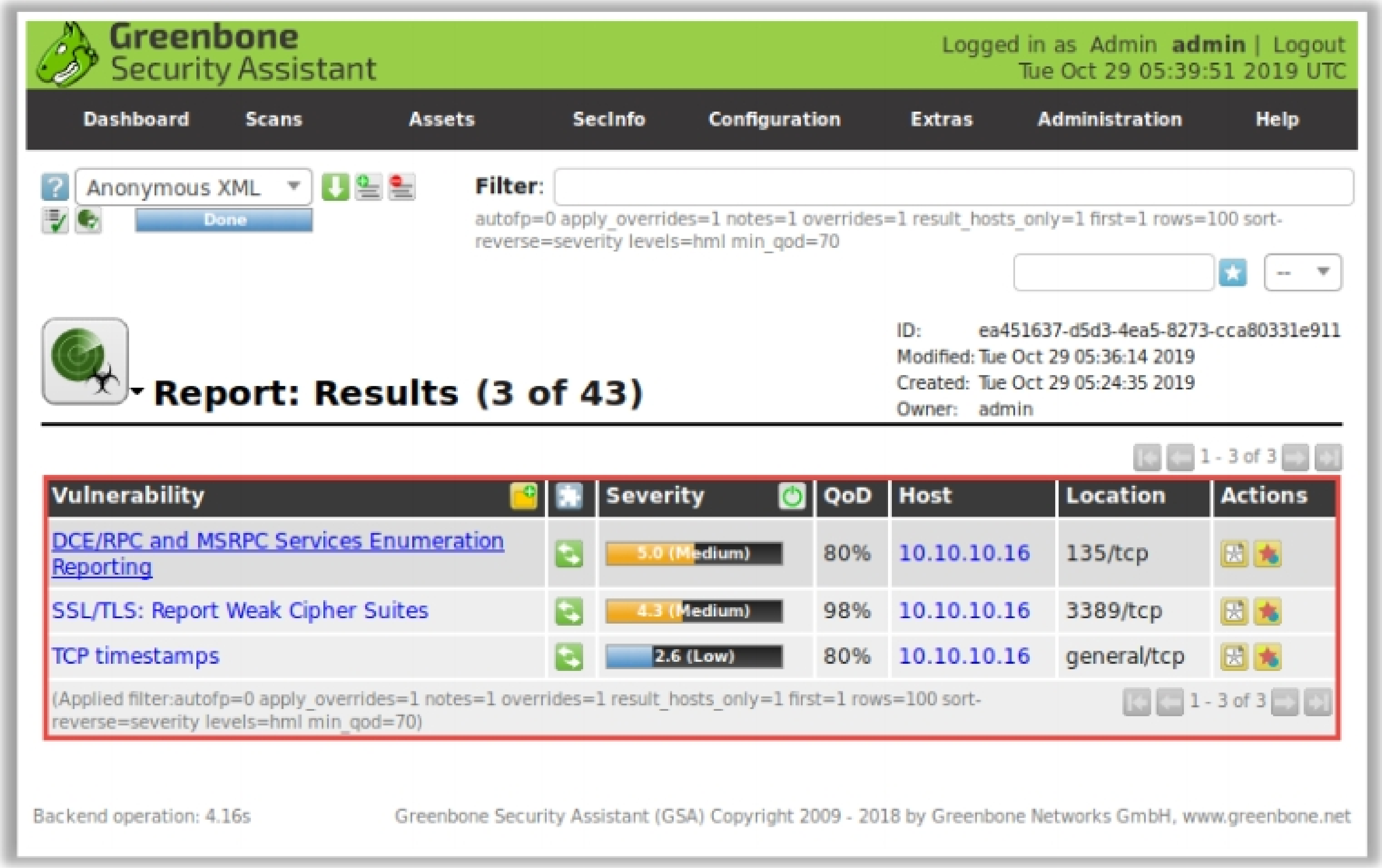
Figure 5.8: Vulnerability scanning using GFI LanGuard

- **OpenVAS**

  Source: *http://www.openvas.org*

  OpenVAS is a framework of several services and tools that offer a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Network's commercial vulnerability management solution, developments from which have been contributed to the open-source community since 2009.

  The actual security scanner is accompanied by a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.



autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (3 of 43)

ID: ea451637-d5d3-4ea5-8273-cca80331e911
Modified: Tue Oct 29 05:36:14 2019
Created: Tue Oct 29 05:24:35 2019
Owner: admin

1 - 3 of 3

Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	10.10.10.16	135/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	10.10.10.16	3389/tcp	
TCP timestamps		2.6 (Low)	80%	10.10.10.16	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 3 of 3

Backend operation: 4.16s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Figure 5.9: Vulnerability scanning using OpenVAS

- **Nikto**

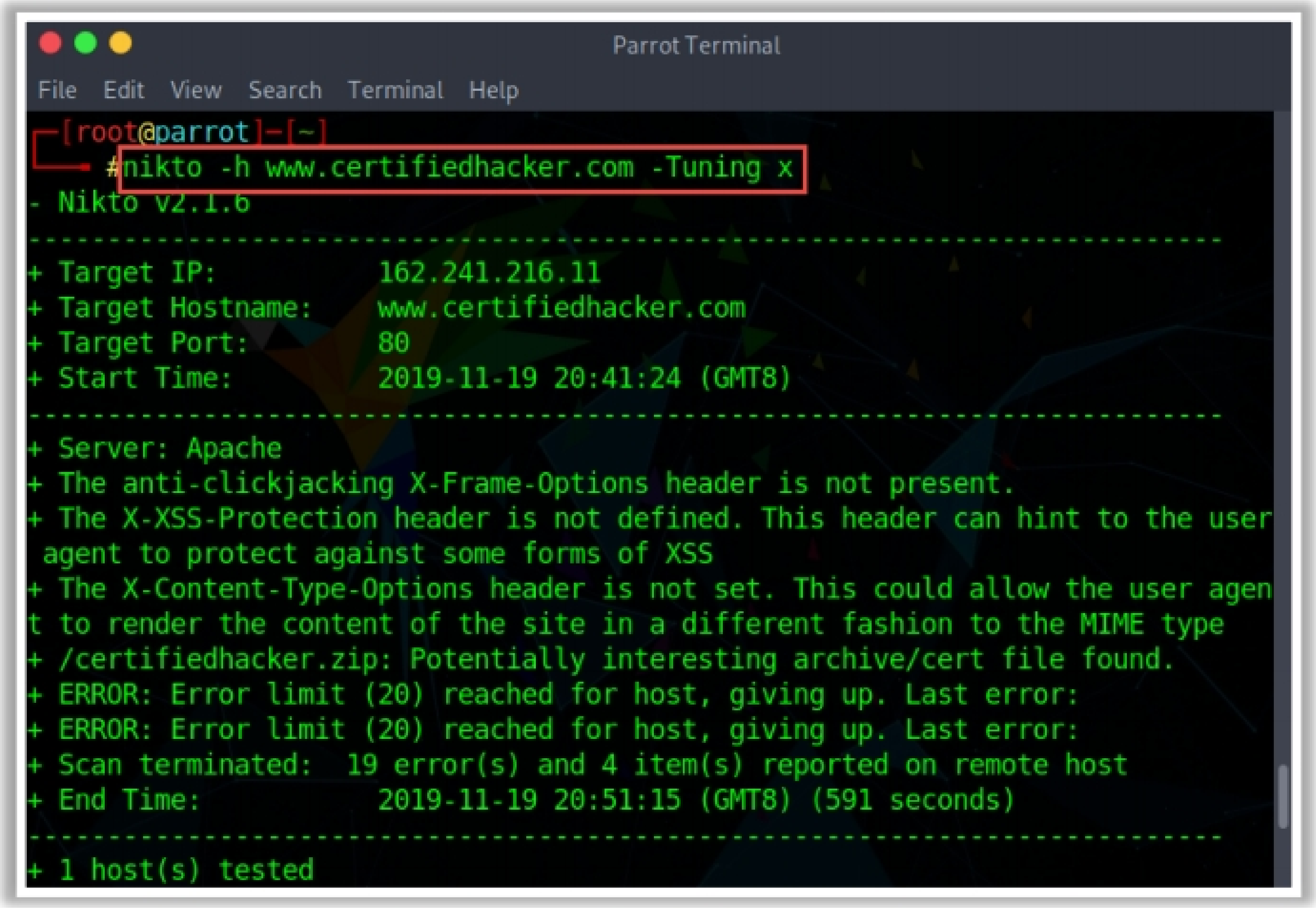
  Source: *https://cirt.net*

  Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files or programs, checks for outdated versions of over 1250 servers, and checks for version specific problems on over 270 servers. It also looks at server configuration items such as the presence of multiple index files and the HTTP server options and will attempt to identify installed web servers and software.

  Features:

  - SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
  - A full HTTP proxy support
  - Checks for outdated server components
  - Saves reports in plain text, XML, HTML, NBE or CSV
  - A Template engine to easily customize reports
  - Scans multiple ports on a server, or multiple servers via input file
  - LibWhisker's IDS encoding techniques
  - Identifies installed software via headers, favicons, and files
  - Host authentication with Basic and NTLM

- Subdomain guessing
- Apache and cgiwrap username enumeration
- Scan tuning to include or exclude entire classes of vulnerability checks
- Guesses credentials for authorization realms (including many default ID and password combinations)

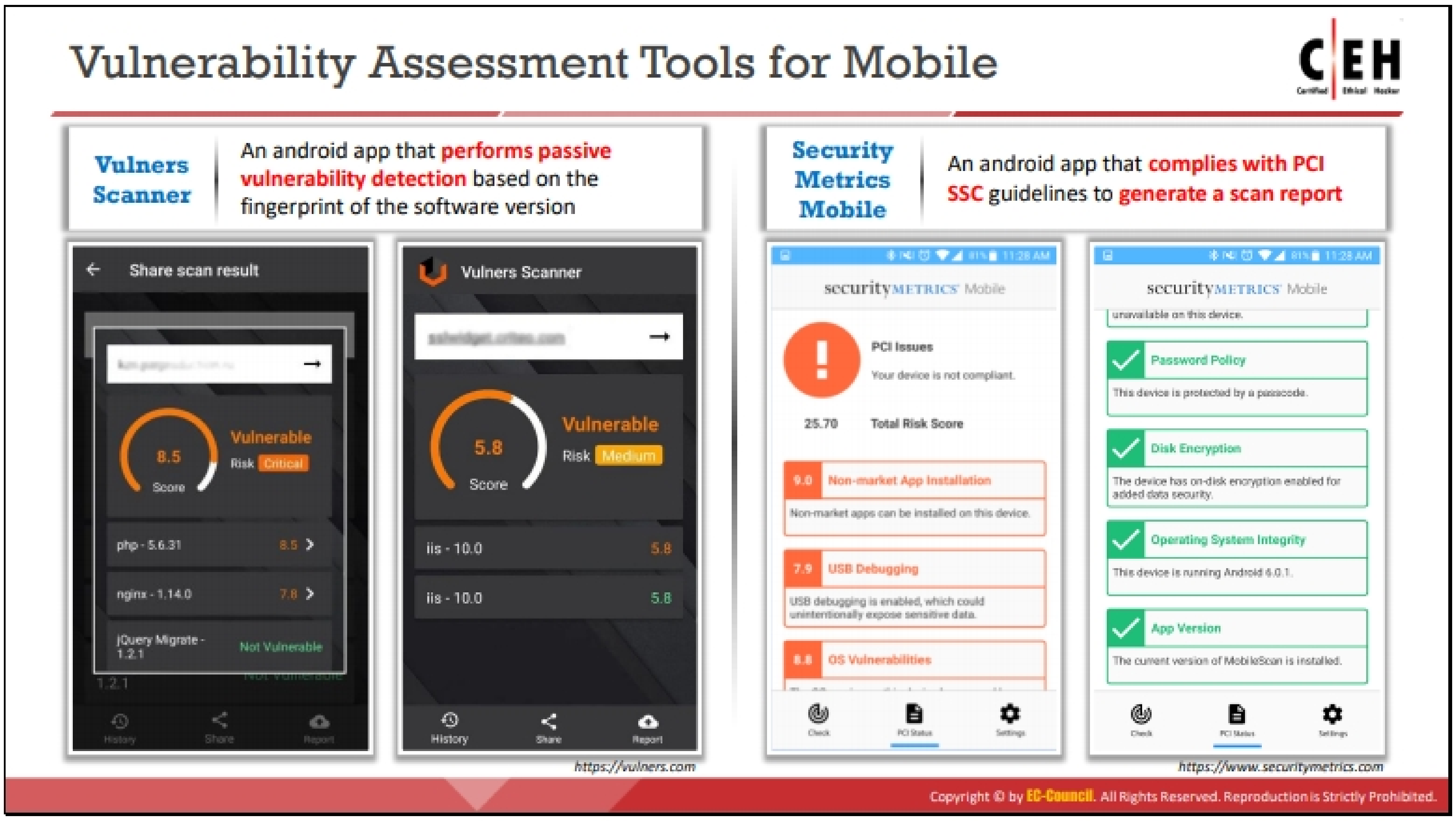


```
┌─[root@parrot]─[~]
└──╼ #nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          162.241.216.11
+ Target Hostname:    www.certifiedhacker.com
+ Target Port:        80
+ Start Time:         2019-11-19 20:41:24 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
 agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agen
t to render the content of the site in a different fashion to the MIME type
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  19 error(s) and 4 item(s) reported on remote host
+ End Time:           2019-11-19 20:51:15 (GMT8) (591 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 5.10: Screenshot of Nikto

Listed below are some of the additional vulnerability assessment tools:

- Qualys FreeScan (*https://freescan.qualys.com*)
- Acunetix Web Vulnerability Scanner (*https://www.acunetix.com*)
- Nexpose (*https://www.rapid7.com*)
- Network Security Scanner (*https://www.beyondtrust.com*)
- SAINT (*https://www.saintcorporation.com*)
- Microsoft Baseline Security Analyzer (MBSA) (*https://www.microsoft.com*)
- beSECURE (AVDS) (*https://www.beyondsecurity.com*)
- Core Impact Pro (*https://www.coresecurity.com*)
- N-Stalker Web Application Security Scanner (*https://www.nstalker.com*)
- ManageEngine Vulnerability Manager Plus (*https://www.manageengine.com*)



Vulnerability Assessment Tools for Mobile

Vulners Scanner — An android app that performs passive vulnerability detection based on the fingerprint of the software version

Security Metrics Mobile — An android app that complies with PCI SSC guidelines to generate a scan report

https://vulners.com

https://www.securitymetrics.com

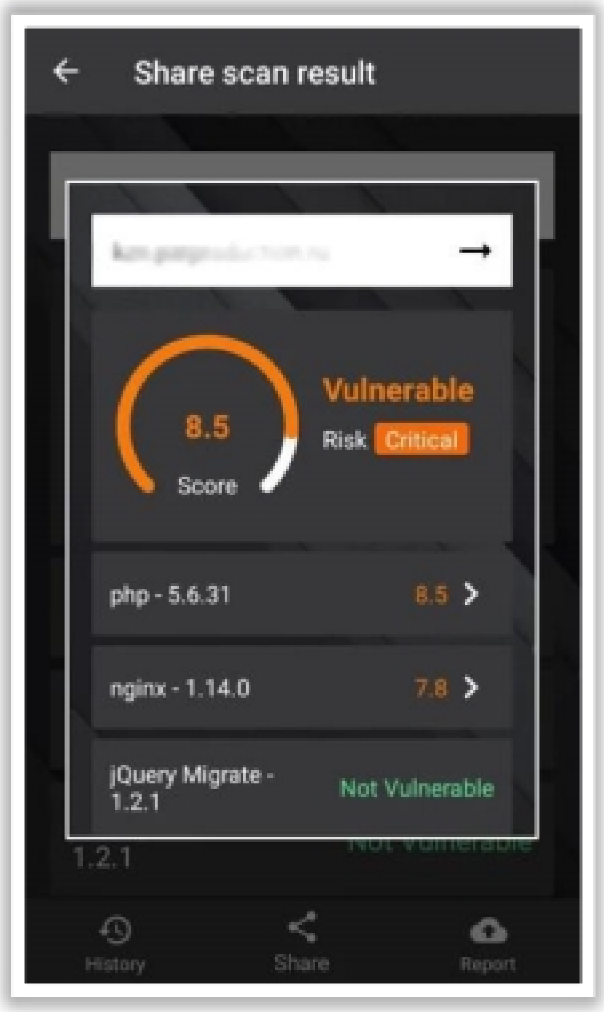
Share scan result
8.5
Score
Vulnerable
Risk
Critical
php - 5.6.31
8.5
nginx - 1.14.0
7.8
jQuery Migrate - 1.2.1
Not Vulnerable
History
Share
Report
Vulners Scanner
5.8
Medium
iis - 10.0
PCI Issues
Your device is not compliant.
25.70
Total Risk Score
Non-market App Installation
Non-market apps can be installed on this device.
USB Debugging
USB debugging is enabled, which could unintentionally expose sensitive data.
OS Vulnerabilities
Password Policy
This device is protected by a passcode.
Disk Encryption
The device has on-disk encryption enabled for added data security.
Operating System Integrity
This device is running Android 6.0.1.
App Version
The current version of MobileScan is installed.
Check
PCI Status
Settings

Vulnerability Assessment Tools for Mobile

- **Vulners Scanner**

  Source: *https://vulners.com*

  Vulners scanner is an android application that performs passive vulnerability detection based on a software version's fingerprint. Since this is a passive method of vulnerability assessment, this app can only be used to identify vulnerabilities; it is not effective in performing compliance checks.



Share scan result
8.5
Score
Vulnerable
Risk
Critical
php - 5.6.31
8.5
nginx - 1.14.0
7.8
jQuery Migrate - 1.2.1
Not Vulnerable
History
Share
Report

Figure 5.11: Vulners Scanner — critical risk score

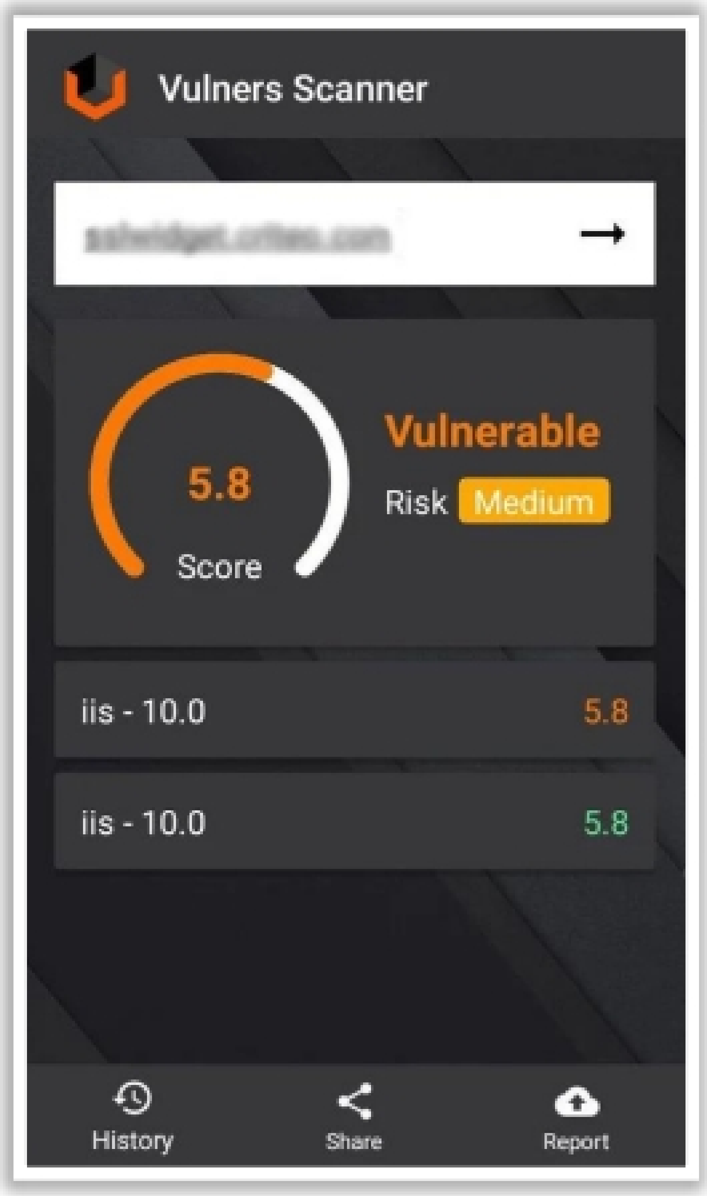


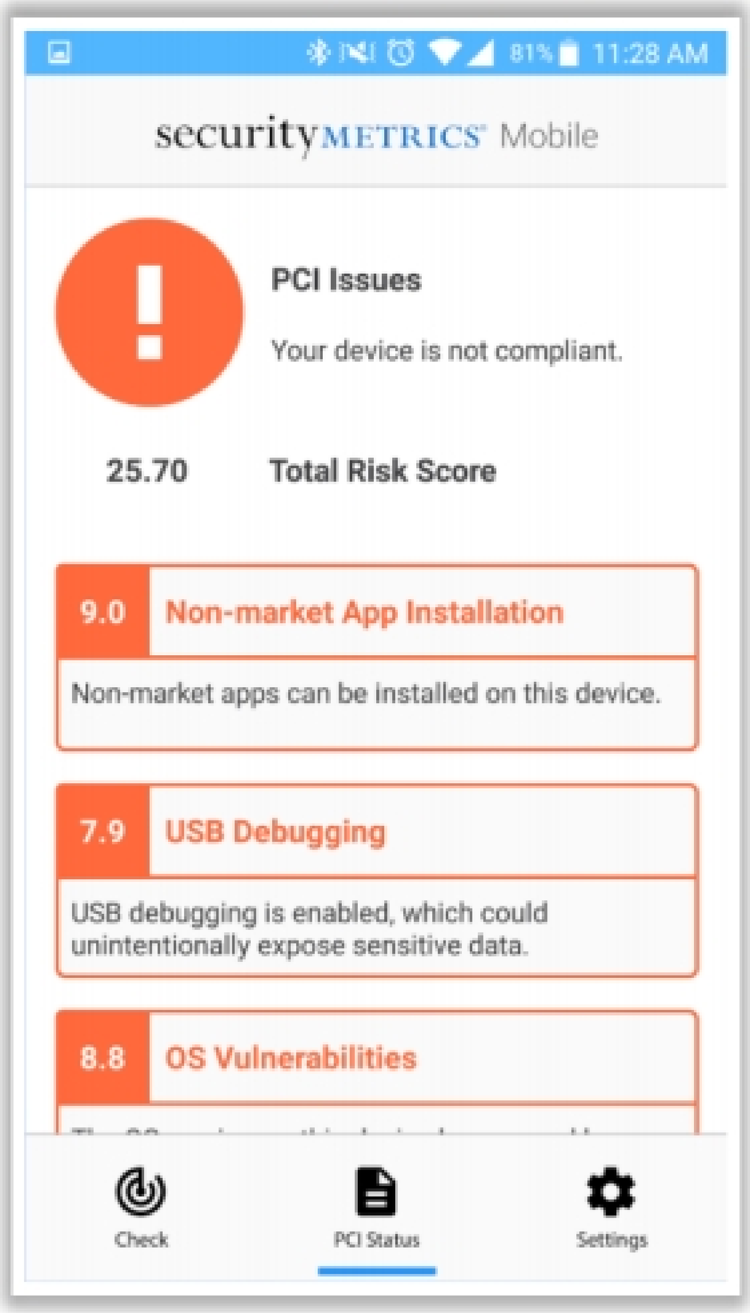
Figure 5.12: Vulners Scanner — medium risk score

- **SecurityMetrics Mobile**

  Source: *https://www.securitymetrics.com*

  SecurityMetrics Mobile is a mobile defense tool that helps to identify mobile device vulnerabilities to protect customers' sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, personal and business use, unwarranted app privileges, data and device storage, account data access, Bluetooth, Infrared (IR), Near-field communication (NFC), and SIM and SD cards.

  SecurityMetrics MobileScan complies with PCI SSC (Payment Card Industry Security Standards Council) guidelines to prevent mobile data theft. On completion of a scan, the report generated comprises a total risk score, a summary of discovered vulnerabilities, and recommendations on how to resolve threats.


81% 11:28 AM
securityMETRICS Mobile
Check
PCI Status
Settings

PCI Issues

Your device is not compliant.

25.70 Total Risk Score

9.0 Non-market App Installation

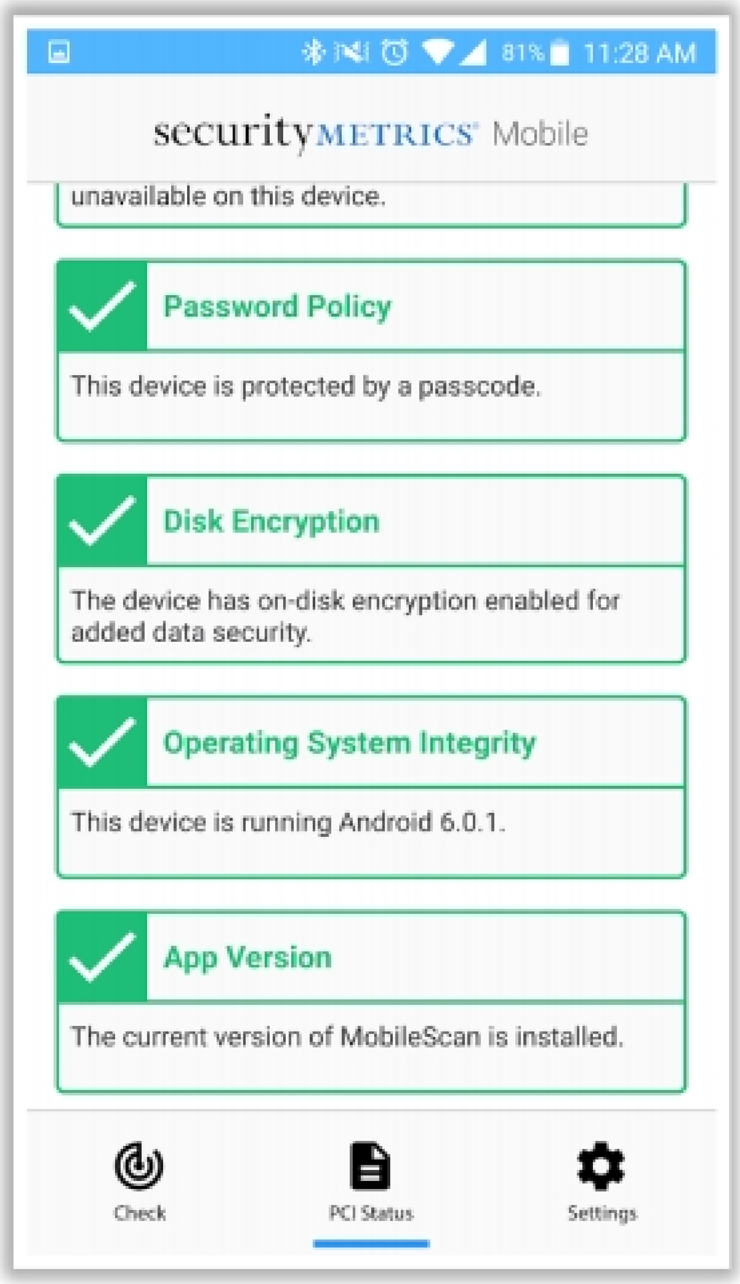
Non-market apps can be installed on this device.

7.9 USB Debugging

USB debugging is enabled, which could unintentionally expose sensitive data.

8.8 OS Vulnerabilities

Figure 5.13: SecurityMetrics Mobile — Risk Score


81% 11:28 AM
securityMETRICS Mobile
Check
PCI Status
Settings

unavailable on this device.

✓ Password Policy

This device is protected by a passcode.

✓ Disk Encryption

The device has on-disk encryption enabled for added data security.

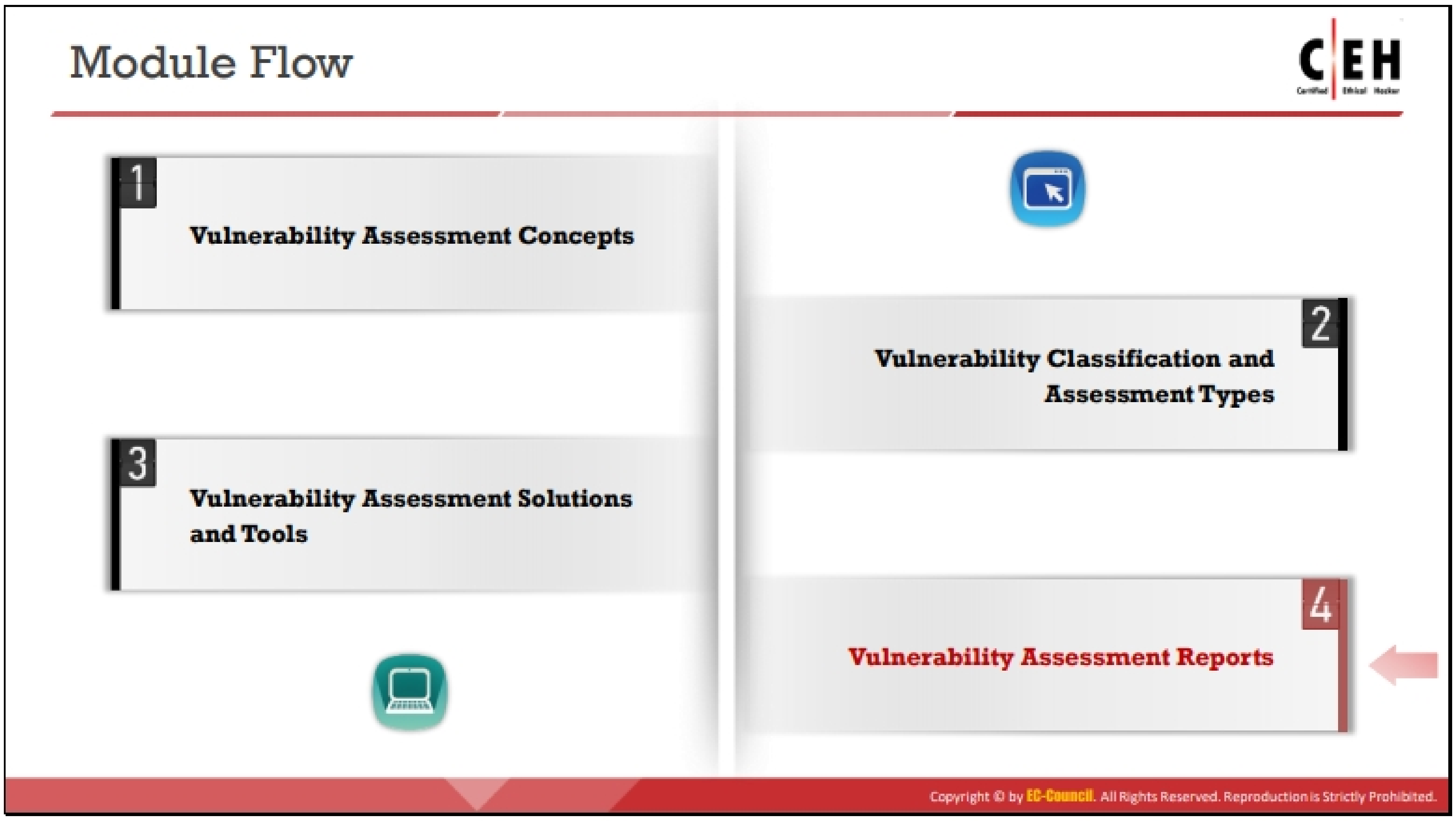
✓ Operating System Integrity

This device is running Android 6.0.1.

✓ App Version

The current version of MobileScan is installed.

Figure 5.14: SecurityMetrics Mobile — result



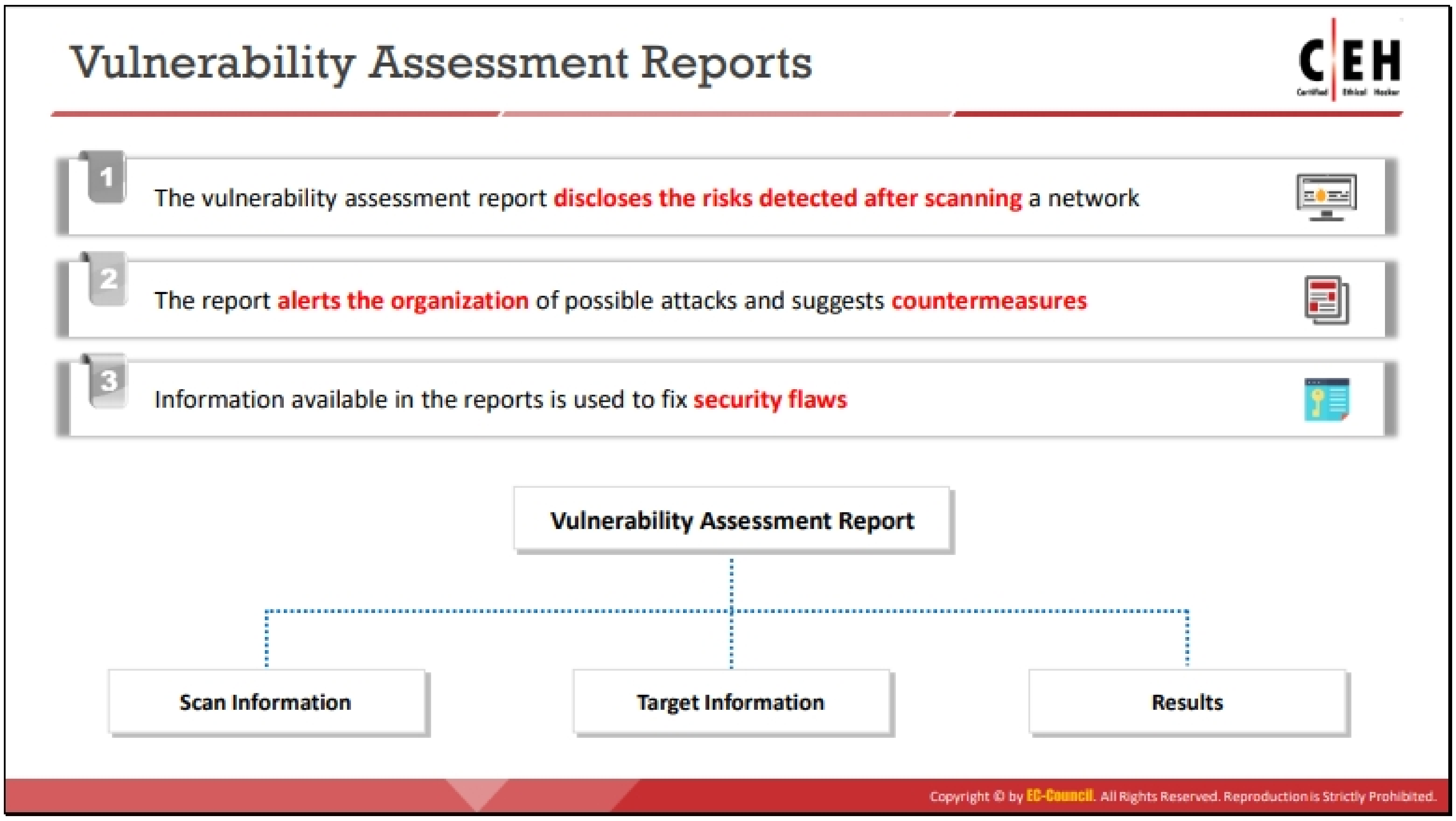
Module Flow

1 **Vulnerability Assessment Concepts**

2 **Vulnerability Classification and Assessment Types**

3 **Vulnerability Assessment Solutions and Tools**

4 **Vulnerability Assessment Reports**



Vulnerability Assessment Reports

1 The vulnerability assessment report **discloses the risks detected after scanning** a network

2 The report **alerts the organization** of possible attacks and suggests **countermeasures**

3 Information available in the reports is used to fix **security flaws**

Vulnerability Assessment Report
Scan Information
Target Information
Results

Vulnerability Assessment Reports

In the vulnerability assessment process, once all the phases are completed, the security team will review the results and process the information to prepare the final report. In this phase, the security team will try to disclose any identified vulnerabilities, document any variations and findings, and include all these in the final report along with remediation steps to mitigate the identified risks.

The vulnerability assessment report discloses the risks that are detected through scanning the network. Tools such as Nessus, GFI LanGuard, and Qualys Vulnerability Management are used for vulnerability assessment. These tools provide a comprehensive assessment report in a specified format. The report alerts the organization to possible attacks and suggests countermeasures.

The report provides details of all the possible vulnerabilities with regard to the company's security policies. The vulnerabilities are categorized based on severity into three levels: High, Medium, and Low risk.

High-risk vulnerabilities are those that might allow unauthorized access to the network. These vulnerabilities must be rectified immediately before the network is compromised. The report describes different kinds of attacks that are possible given the organization's set of operating systems, network components, and protocols.

The vulnerability assessment report must include, but are not limited to, the following points:

- The vulnerability's name and its mapped CVE ID
- The date of discovery
- The score based on Common Vulnerabilities and Exposures (CVE) databases
- A detailed description of the vulnerability
- The impact of the vulnerability
- Details regarding the affected systems
- Details regarding the process needed to correct the vulnerability, including information patches, configuration fixes, and ports to be blocked.
- A proof of concept (PoC) of the vulnerability for the system (if possible)

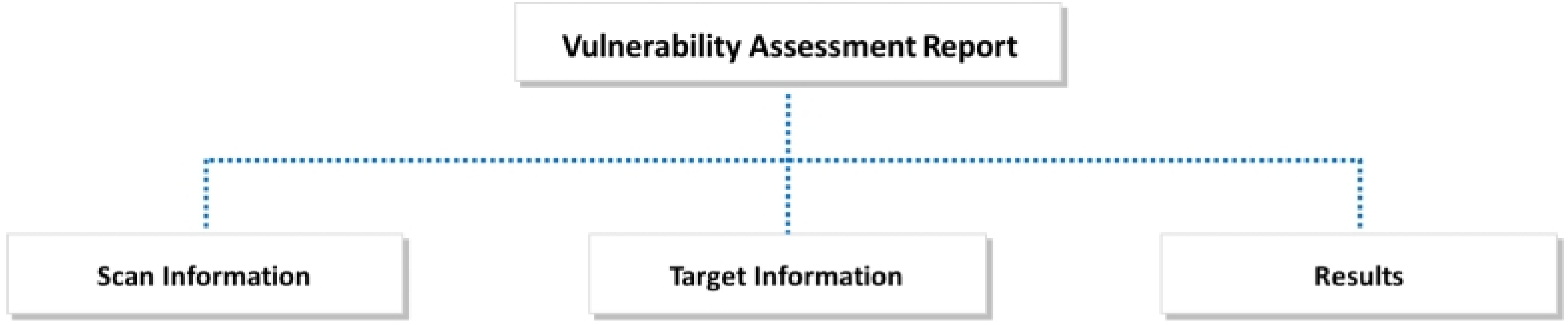
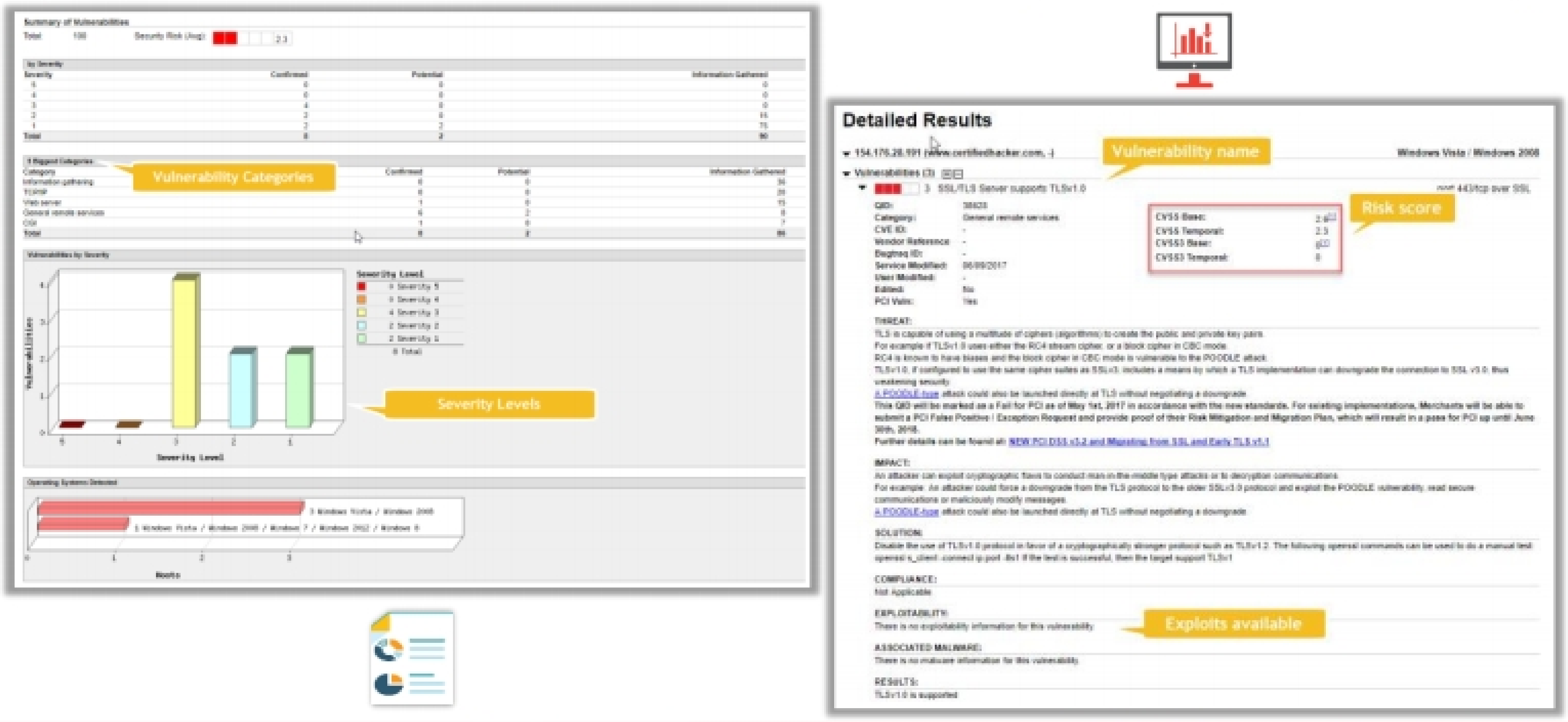


Figure 5.15: Components of a vulnerability assessment report

Analyzing Vulnerability Scanning Report



Analyzing Vulnerability Scanning Report

A vulnerability assessment report provides detailed information on the vulnerabilities found in the computing environment. The report helps organizations identify the security posture of the computing systems (such as web servers, firewalls, routers, email, and file services) and provide solutions to reduce system failures. An ethical hacker must be careful in analyzing the vulnerability assessment reports to avoid false positives.

The assessment report helps organizations to take mitigation steps to proactively avoid risk by identifying, tracking, and eliminating security vulnerabilities.

Vulnerability reports cover the following elements:

- **Scan information**: Provides information such as the name of the scanning tool, its version, and the network ports to be scanned.
- **Target information**: Contains information about the target system's name and address.
- **Results**: A complete scanning report containing subtopics such as target, services, vulnerability, classification, and assessment.
- **Target**: Includes each host's detailed information and contains the following information:
    - **<Node>**: Contains the name and address of the host
    - <**OS**>: Shows the operating system type
    - **<Date>**: Gives the date of the test
- **Services**: Defines the network services by their names and ports.
- **Classification**: Allows the system administrator to obtain additional information about the scan, such as its origin.

- **Assessment**: Provides information regarding the scanner's assessment of discovered vulnerabilities.

Vulnerability assessment reports are classified into two types:

- Security Vulnerability Reports
- Security Vulnerability Summaries

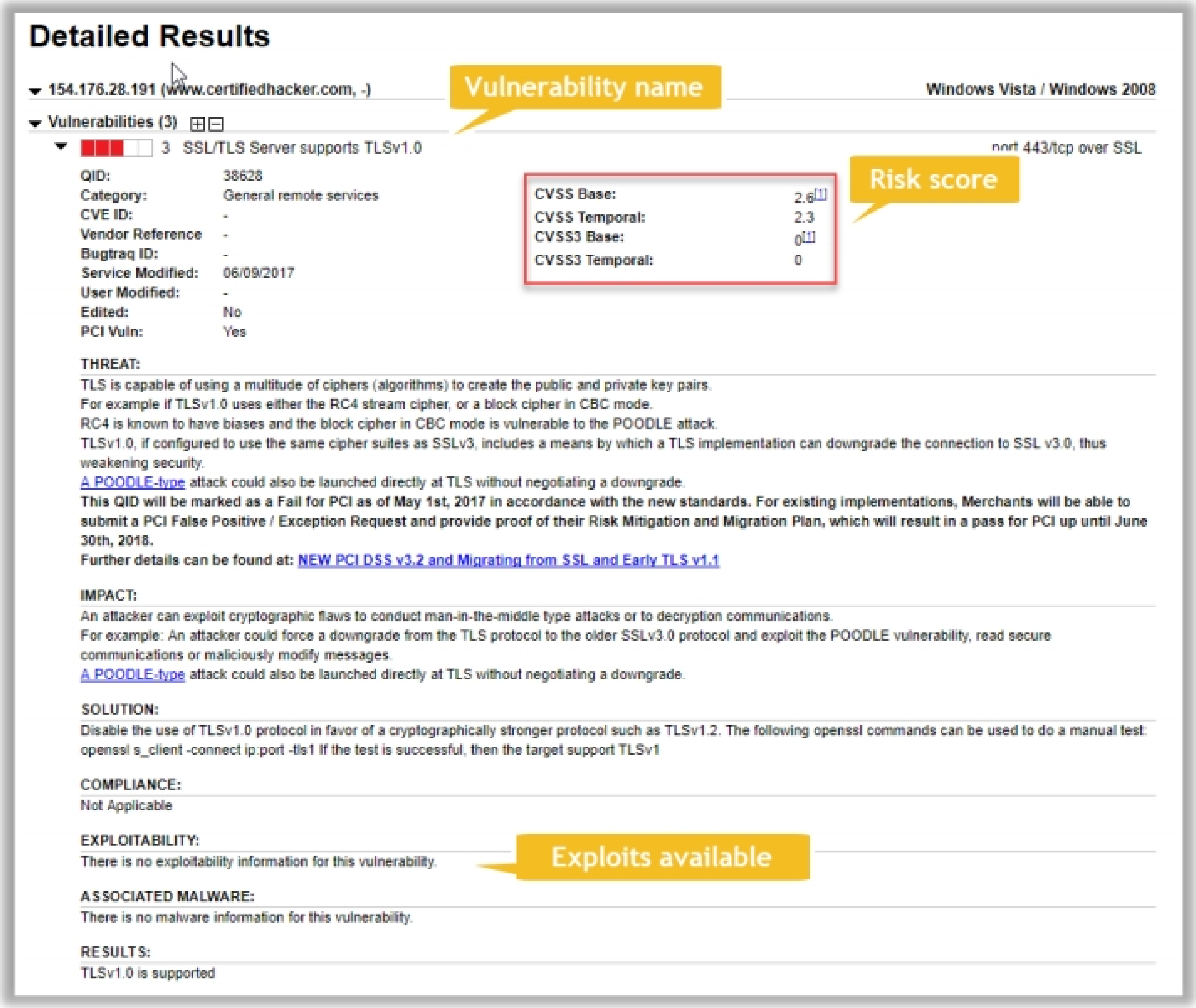
Security Vulnerability Report

This is a combined report for all the scanned devices and servers in the organization's network.

The security vulnerability report includes the following details:

- Newly found vulnerabilities
- Open ports and detected services
- Suggestion for remediation
- Links to patches

A sample security vulnerability report is as follows:



Detailed Results

154.176.28.191 (www.certifiedhacker.com, -) Windows Vista / Windows 2008

Vulnerabilities (3)

3 SSL/TLS Server supports TLSv1.0 port 443/tcp over SSL

QID: 38628
Category: General remote services
CVE ID: -
Vendor Reference -
Bugtraq ID: -
Service Modified: 06/09/2017
User Modified: -
Edited: No
PCI Vuln: Yes

CVSS Base: 2.6[1]
CVSS Temporal: 2.3
CVSS3 Base: 0[1]
CVSS3 Temporal: 0

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.
This QID will be marked as a Fail for PCI as of May 1st, 2017 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018.
Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:
Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test:
openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

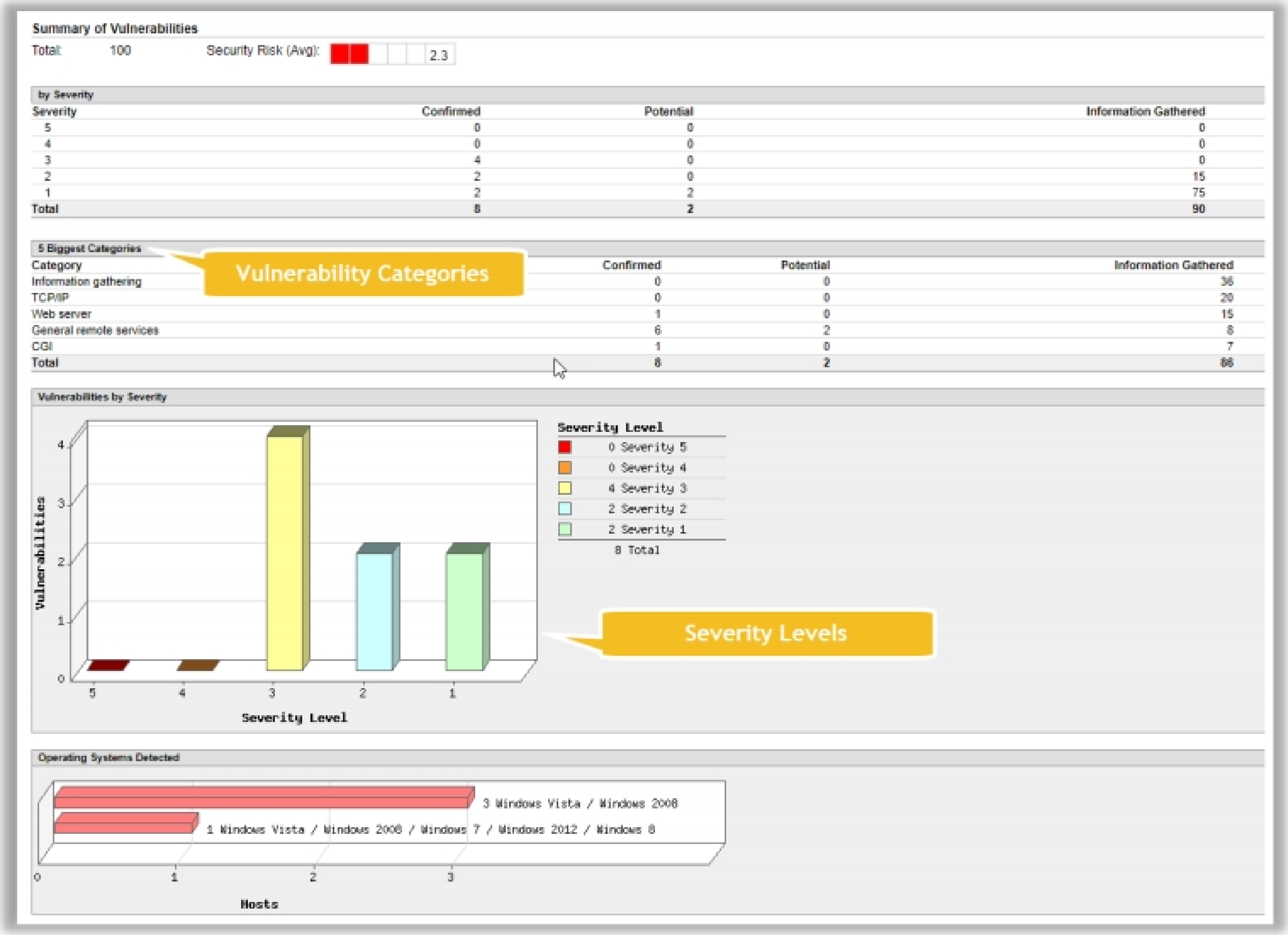
RESULTS:
TLSv1.0 is supported

Figure 5.16: Security vulnerability report

Security Vulnerability Summary

This report is produced for every device or server after scanning. It gives a summary of the scan result that includes the following elements:

- Current security flaws
- Categories of vulnerabilities
- Newly detected security vulnerabilities
- The severity of vulnerabilities
- Resolved vulnerabilities



Summary of Vulnerabilities

Total: 100 Security Risk (Avg): 2.3

by Severity

Severity	Confirmed	Potential	Information Gathered
5	0	0	0
4	0	0	0
3	4	0	0
2	2	0	15
1	2	2	75
Total	**8**	**2**	**90**

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered
Information gathering	0	0	36
TCP/IP	0	0	20
Web server	1	0	15
General remote services	6	2	8
CGI	1	0	7
Total	**8**	**2**	**86**

Vulnerability Categories

Vulnerabilities by Severity

Vulnerabilities
0
1
2
3
4
5
4
3
2
1
Severity Level

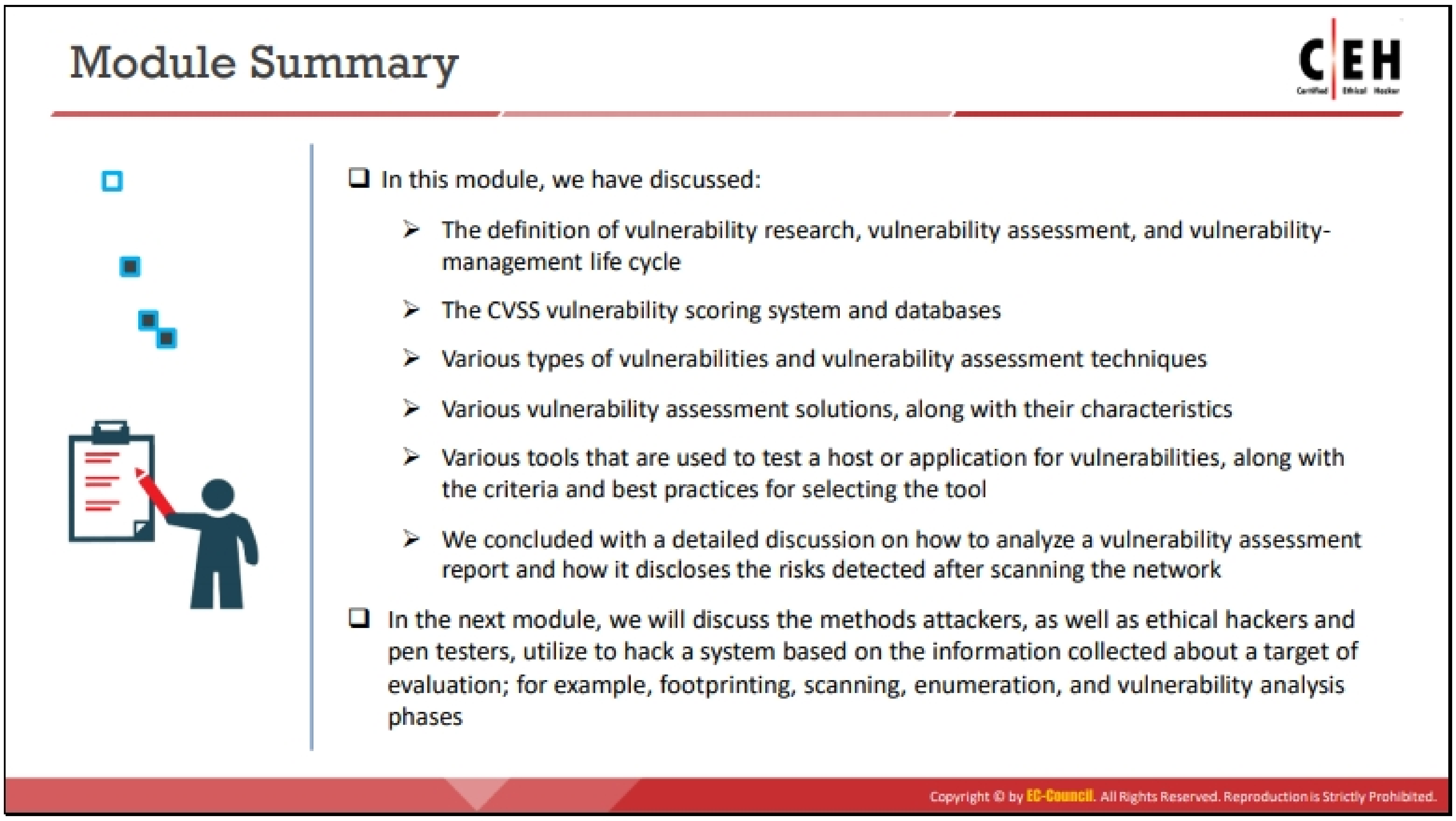
Severity Level	
🟥	0 Severity 5
🟧	0 Severity 4
🟨	4 Severity 3
🟦	2 Severity 2
🟩	2 Severity 1
	8 Total

Severity Levels

Operating Systems Detected

3 Windows Vista / Windows 2008
1 Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8
0
1
2
3
Hosts

Figure 5.17: Security vulnerability summary



Module Summary

- ☐ In this module, we have discussed:
  - ➢ The definition of vulnerability research, vulnerability assessment, and vulnerability-management life cycle
  - ➢ The CVSS vulnerability scoring system and databases
  - ➢ Various types of vulnerabilities and vulnerability assessment techniques
  - ➢ Various vulnerability assessment solutions, along with their characteristics
  - ➢ Various tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool
  - ➢ We concluded with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning the network
- ☐ In the next module, we will discuss the methods attackers, as well as ethical hackers and pen testers, utilize to hack a system based on the information collected about a target of evaluation; for example, footprinting, scanning, enumeration, and vulnerability analysis phases

Module Summary

This module discussed vulnerability research, vulnerability assessment, and the vulnerability-management life cycle. It also discussed the CVSS vulnerability scoring system and databases and various types of vulnerabilities and vulnerability assessment techniques. It described various vulnerability assessment solutions along with their characteristics and described various vulnerability assessment tools that are used to test a host or application for vulnerabilities, along with the criteria and best practices for selecting the tool. Finally, this module ended with a detailed discussion on how to analyze a vulnerability assessment report and how it discloses the risks detected after scanning a network.

The next module will show how attackers, as well as ethical hackers and pen testers, attempt system hacking based on the information collected about a target in the footprinting, scanning, enumeration, and vulnerability analysis phases.